Assurance of the Geneva E2E-VIV Protocol and System

Free & Fair
February 2017

Executive Summary

Free & Fair is pleased to offer to the Canton of Geneva services and development work to ensure that their end-to-end verifiable Internet voting system fully conforms to all provisions set forth in the Federal Chancellery Ordinance on Electronic Voting. Our proposal is for an eight calendar month period of performance (circa 15 April to 15 December 2017), our effort estimate for the work is 72 man weeks (18 man months) of work, and our total budget for the work is $812,000. Incidentals, flights, and hotel costs for visits to the client are not included in this price. We describe the offer with a staged approach, focusing on work packages, milestones, and deliverables whose value and utility can be separately evaluated, and consequently separately budgeted.

Few organizations in the world have expertise close to ours in these matters. We have accomplished, always on-time and on-budget, many pieces of comparable work over past two decades. Our past R&D work has been for many demanding clients, including several foreign governments and many branches of the U.S. Federal Government. We summarize some of that past work herein and are happy to provide references.

In this proposal, in particular, we offer to:

- formally specify using domain engineering the domain elements of the Swiss context informally specified in the Federal Act on Political Rights (“PoRA” henceforth), the Ordinance on Political Rights (“PoRO” henceforth), the Federal Chancellery Ordinance on Electronic Voting (“VEleS” henceforth), and the Technical and the Administrative Requirements for Electronic Vote Casting Annex (“the Annex”, henceforth). This work ensures that there exists a uniform, semantically unambiguous formal model of End-to-End Verifiable Internet Voting (“E2E-VIV”, henceforth) in the Swiss context;
- formally specify the requirements of any E2E-VIV system that fulfills the mandates set forth in these documents;
- perform a formal threat analysis, risk analysis, and assessment based upon this domain engineering and set of requirements;
- formally specify the cryptographic protocol and algorithms semi-formally described in the *chVote System Specification* by Haenni, Koenig, and Locher;
- formally verify all correctness and security properties of the chVote protocol; and
- provide consultancy to the authorities on matters relating to the state-of-the-art in:
  (a) building an assurance case for an implementation of the protocol;
  (b) formal specification and reasoning about protocol, algorithms, and systems;
  (c) rigorous engineering methods and tools, particularly those that are correct-by-construction for the trusted computing base of the chVote system;
  (d) techniques through which expensive computations can be distributed in a secure, privacy-preserving fashion; and
  (e) matters of usability and accessibility, especially in the context of E2E-VIV.

Free & Fair
http://freeandfair.us
421 SW 6th Ave., Suite 300
Portland, Oregon 97204
T 971.808.3247
F 503.350.0933

This latter offer of consultancy may lead to further collaboration with the Canton of Geneva on several topics, including the development of a high assurance verifier of trace-based proofs generated by each execution of the protocol, the development of a distributed client- or server-side of the system in order to have a more efficient and usable privacy-preserving voting system, and the formal verification of the trusted computing base of the chVote system (its so-called “control components”).

All formal specification and verification work will be accomplished in a mechanized fashion, using the latest state-of-the-art tools for specifying and reasoning about cryptographic primitives and protocols. Our work is akin to the by-hand cryptographic proofs by Shoup and Gjøsteen cited by authorities, but updated to the modern context. Furthermore, because the proofs are machine assisted and machine checked, they cannot and will not have the flaws, omissions, and elisions common in the cryptographic literature.

The end result of the work will be a “literate” book that can be read and peer-reviewed by both a human and software. This specification can also be used to provide a formal assurance case about some or all of a rigorously engineered implementation of the system. In particular, using these specification artifacts, one can formally validate and verify implementations of the trusted computing base of the chVote system.

Free & Fair

Free & Fair’s mission is to bring open source, high-assurance, end-to-end verifiable elections to the world.[1]

Free & Fair is exactly the right entity to realize the Canton of Geneva’s vision because we have:

- world-class expertise in high assurance open source elections systems;
- world-class expertise in E2E-VIV systems, given that we are the authors of the de facto global standard on the requirements—including the necessary underlying technology and cryptography—of such systems;[2]
- an unparalleled record in delivering high assurance tools and systems to the most demanding clients in the USA on time and within budget;
- deep experience in the mechanical specification and verification of cryptographic algorithms and protocols, including those related to E2E-VIV systems;
- vast experience with creating, contributing to, and managing Open Source Software, and a deep knowledge of Open Source licenses and business cases; and
- corporate principles that focus on transparency, security, and affordability.

[1] Galois, Inc. produces hardware and software for a variety of applications. For election-related products, Galois operates under the name Free & Fair.
[2] See the U.S. Vote Foundation’s report *The Future of Voting: End-to-End Verifiable Internet Voting—Specification and Feasibility* available via https://www.usvotefoundation.org/e2e-viv/summary

Our world-class expertise is concretized in five main dimensions relevant to the Canton of Geneva:

- Free & Fair has, in aggregate, nearly 100 years of open source experience spanning over 100 open source projects, including experience resolving the security issues raised by use of COTS hardware.
- Free & Fair has, in aggregate, many dozens of years of expertise in formally specifying and verifying cryptographic algorithms, protocols, and implementations for demanding federal and private industry clients.
- Free & Fair staff have been involved with, or are the originators of, some of the most influential, high-profile open source projects in the world. The breadth of our work is remarkable, and includes the world's most popular operating system (Linux, used in Android phones and many other consumer electronics devices), libraries for secure communication and storage (e.g,. SSL libraries and cryptography on many recent LG smartphones), programming languages (e.g., Java, Fortran, and Eiffel), programmer tools (e.g., Emacs, Eclipse, and numerous plugins to modern IDEs), compilers (e.g., the GNU compiler toolchain and the clang/LLVM toolchain), graphics (e.g., Mesa, the library which provides 3D rendering on many platforms), and a plethora of tools used for teaching about and building high assurance systems (OpenJML, ESC/Java2, EBON, Cryptol, SAW, and more).
- Our CEO and Chief Scientist, Dr. Joseph Kiniry, is widely known in the elections integrity and scientific community for his fifteen years of work pursuing a vision of high assurance election systems for trustworthy democracy.
- Free & Fair is already deeply familiar with elections technology, and E2E-VIV systems in particular. During Dr. Kiniry's tenure as an academic in The Netherlands, the Republic of Ireland, and Denmark, his research group examined and critiqued several Internet Voting (IV) systems. Due to that work—analyzing the quality of implementations and reasoning about the correctness of their protocols—experiments in IV in The Netherlands (the Nedap system and the KOA IV system), the Republic of Ireland (the Nedap and Powervote systems), experiments in IV in Norway and Estonia, and investigations into digital elections in Denmark were significantly impacted. During those time frames, he directly consulted with those governments and their expert working groups, provided public guidance on matters relating to the deployment of digital election systems, educated the public about the opportunities and challenges of digital elections, and advocated for election integrity.

Another strength is our ability to attract and manage world-class subcontractors. We commonly work with world-class firms, small and large, as well as top universities in achieving our ambitious research, development, and engineering goals.

On Time and Within Budget

Free & Fair's principals and this project team have ample experience delivering provably secure technology to government and industry clients, on time and within budget. We can provide information about a large set of projects that were delivered on time and within budget.

We have also implemented deployed high assurance election systems. An early example of such is the election tabulation system built by a team led by Dr. Kiniry for use by The Netherlands in the 2004 European Council Elections. This system was developed and certified within 12 calendar weeks instead of the year or more typical for election systems in that country at that time.[3]

Open Source Veterans

Traditionally, election technology vendors have profited from limited competition and retaining ownership of proprietary systems. Free & Fair has a different business model. We understand the budget constraints that countries and jurisdictions face, and welcome the opportunity to be a partner in finding ways to control costs by using COTS hardware and open source software, allowing competition into every aspect of election technology.

In particular:

- All software source code, related software engineering artifacts, and proof engineering artifacts that we have developed and that we propose to the client are open source, which allows inspection by any person interested in assuring or improving the security or functions of the voting system.
- All hardware proposed is either COTS or, where custom hardware is required, open hardware, allowing clients to benefit from open competition among vendors.
- All software that we develop, and nearly all verification work that we do, can be made to run on all mainstream operating systems (Microsoft Windows, Apple OS X, and various Linux flavors).

Security for "Critical Infrastructure"

In preparation for the 2016 U.S. Presidential election, nearly every state requested help from the U.S. Department of Homeland Security (DHS) to secure election technology. Events such as these requests, and inquiries following the election, have raised public awareness of the importance of security to election administration. Even without a malicious attack, every Election Day brings stories of bugs and glitches that cause a public outcry somewhere, especially if the number of votes affected comes close to a margin of victory. More than ever before, election officials have been asked to assure the public that their elections have been run correctly. In

[3] For more detail, see the Methodology section of 5.7 below.

January 2017, in response to the increasing sophistication of adversaries who might wish to attack or disrupt U.S. elections, the DHS officially designated U.S. elections systems "critical infrastructure" on par with systems vital to energy, financial services, healthcare, transportation, agriculture, and communications.

Free & Fair has treated democracy and election systems as critical systems and infrastructure for decades in our work with other governments and in R&D projects on election systems. We propose to build election technology for the Canton of Geneva that meets the highest standards for software design and security, such as those stipulated by the U.S. National Institute of Standards and Technology (NIST) and similar agencies in Switzerland. Most common commercial computing systems depend on "recovery" from occasional crashes (if the screen freezes, just restart it!), but the software development techniques specified by NIST have proven effective for building software **without bugs**. While these techniques may be new to the election community, key members of the Free & Fair project team have used them for 17 years in government contracts totalling over $160M. We have developed products for governments and secured those products against persistent threats from nation-state actors (such as Russia or North Korea) and insider attacks. Free & Fair proposes not merely to fulfill the the Canton of Geneva requirements, but to fulfill the requirements with systems as secure as the other systems currently designated "critical infrastructure" by DHS and comparable Swiss agencies.

NIST Special Publication 800-160[4] specifies **high-assurance systems**, also known as **trustworthy systems**. These systems are designed from first principles to be free of flaws. These include flaws related to system correctness, security, reliability, assurance, and more. High-assurance systems are used in situations where failure can lead to loss of life (e.g., an automated train) or have enormous financial implications (e.g., digital cash in smart cards).

Free & Fair project team members have successfully developed many high assurance systems that face many of the same challenges (correctness, security, usability, accessibility, etc.) and use the same technologies (operating systems, programming languages, distributed systems, cryptography, etc.) required by elections systems. Our development process and methodology—cited prominently in NIST Interagency Report 8151,[5] written for the White House—includes strict adherence to design, code, and documentation standards, provides easily verifiable evidence for implementation correctness and security, and incorporates the writing and generation of comprehensive test suites for every component of the system. Free & Fair will bring the high assurance of safety and mission-critical systems to the elections systems and services market, at low cost, and with publicly owned open source technology on COTS hardware.

[4] NIST Special Publication 800-160: *Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, https://doi.org/10.6028/NIST.SP.800-160
[5] NIST Interagency Report 8151: *Dramatically Reducing Software Vulnerabilities,* https://doi.org/10.6028/NIST.IR.8151

Deployment Track Record

Over the past fifteen years, Free & Fair staff members have consistently created and supported critical technology products. We have a track record of productizing, deploying, and continuously maintaining complex, secure, high-assurance technologies. Some of the highlights that illustrate our history of deploying and maintaining highly advanced, often open source systems, used by some of the biggest organizations in the world include:

- **High Assurance Cyber Military Systems (HACMS):** Tools to generate provably secure code for vehicles. Used by Boeing to "hack-proof" the unmanned Little Bird.
- **CyberChaff:** Advanced network defense system that leverages distraction and obfuscation. Deployed by a Fortune 50 company and at universities.
- **Copilot:** Software to detect and report critical hardware failures before they cause accidents. Funded and deployed at NASA.
- **Cryptol:** Toolset to create and verify encryption software. Funded by NSA and deployed across US government.
- **Software Analysis Workbench:** Toolset to help scientists and engineers formally verify computer programs and establish provable correctness and security guarantees. Deployed by Amazon to provably guarantee the correctness of encryption software.

Period of Performance and Effort Estimates

Given the schedule summarized by the Security and Economy Department (DSE), our proposed period of performance for this project is circa 15 April 2017 to 15 December 2017, an eight calendar month interval. Given the final target date of the DSE (15 December 2017), this project can start no later than 24 April 2017 to meet the DSE's schedule objectives. Later starts imply later completions, as the work cannot be parallelized to a great degree and the number of experts who have the skill set necessary to accomplish this work, even globally, is very small.

We have performed an effort estimate, based upon our long experience in running similar projects, for every task in our project plan. Consequently, using an automatically generated set of estimated performer assignments, we have deduced a performer cost for every task. Scientific and project leadership is spread across the entire project in an appropriate proportional fashion for pricing. Thus, the total price for each task corresponds to the necessary scientific and operational activities of that task. We are happy to provide our detailed project planning information to the Canton of Geneva upon request.

In order to successfully execute on the estimated 72 man weeks of work in eight calendar months, we estimate that we will need to devote a fraction of the time of sixteen staff—four cryptographers, nine formal methods experts, one project lead, and one scientific lead—to accomplish all the deliverables of our full proposal. If the client chooses a subset of deliverables, there will be an appropriate corresponding reduction in staff and cost.

Free & Fair
http://freeandfair.us
421 SW 6th Ave., Suite 300
Portland, Oregon 97204
T 971.808.3247
F 503.350.0933

Statement of Work

The Statement of Work consists of four main components with several subcomponents. Our offer of consultancy for the duration of the project constitutes a fifth, optional, component. Follow-on work focusing upon distributed computation, assurance cases, the implementation of a high assurance trusted computing base, and similar are *not included* in this statement of work. Accomplishing those objectives entails a new proposal, statement of work, and budget.

I. **Project State and Foundations.**
At project start the underlying legal, policy, and operational context of the chVote system are read and understood by our performers working in tandem with domain experts within the Canton of Geneva. *Domain engineering* is used to formalize domain elements informally described within the PoRA, PoRO, VLIeS, and Annex, along with any other relevant documents provided by the authorities.[6] This work ensures that there exists a uniform, semantically unambiguous formal model of E2E-VIV in the Swiss context. We also formally specify the requirements of any E2E-VIV system that fulfills the mandate set forth in these documents (the PoRA, etc.).

We formalize such domain models and requirements in a combination of the Galois System Specification Language (GSSL, a variant of the Extended BON[7] system specification language) and a Higher Order Logic (HOL) framework, such as Coq or PVS.[8]

II. **Threat Analysis, Risk Analysis, and Assessment.**
Based upon that foundation, we perform a threat analysis, risk analysis, and assessment of the context of the system as deployed in the modern world. We take into account the current state of cybersecurity threats and threats to system development, operation, deployment and maintenance. We also provide an interactive model upon which evidence-based decisions can be made with regards to the evolving threat landscape.

This work is also formalized in GSSL and a logical framework. Automated reasoning about threats is performed by automated solvers, such as SAT and SMT solvers, and automated deduction of threats is performed by mathematical reasoning systems, such as Mathematica, Matlab, Maple, Magma, SageMath, etc.

---

[6] We perform domain engineering in the style of Dines Bjørner, as described in his extensive notes on such ("Domain Engineering" published in Springer's Formal Methods 2010) and his EATCS Series *Software Engineering Vols. 1–3* published by Springer.
[7] See *Seamless Object Oriented Software Architecture: Analysis and Design of Reliable Systems* by Kim Waldén and Jean-Marc Nerson and *Kind Theory* by Joseph Kiniry.
[8] See https://coq.inria.fr/ and http://pvs.csl.sri.com/

III. **Mechanization.**

Based upon the formal domain model, we next mechanize the chVote protocol, including all cryptographic elements/algorithms upon which it depends. Since the Canton wants both computational and symbolic proofs of security, we propose to use a sensible combination of technologies for this reasoning and proof engineering.

While we have expertise in several such systems, we propose to use a combination of the Cryptol, ProVerif, CryptoVerif, and F* tool suites.[9]

Moreover, the resulting specifications can be leveraged in many ways, including:

A. automated generation of runtime verification test benches for algorithms, protocol, subsystem, integration, and system testing;
B. formal verification of high performance cryptographic algorithms used as primitives in the protocols (using the Cryptol and SAW[10] tools);
C. formal assurance of hand-written implementations of protocols using a combination of a systematic testing framework for the protocol (a la FlexTLS[11]), a trace-based bisimulation testing approach, and the formal verification of the implementation itself (using tools such as SAW, Frama-C[12], OpenJML[13], and similar, depending upon the implementation language chosen by the Canton);
D. easy re-running of verifications against, and providing of feedback about, new variants of the protocol proposed to counter new threats, optimize for performance, or conform to new regulations;
E. automated generation of an implementation of some or all of the protocol (e.g., through the use of the compilation/synthesis backends of the tools); and
F. performing formal regression validation and verification and, if warranted, certification of alternative implementations of the system or its subcomponents, as the system evolves in the future.

IV. **Proof Engineering.**

Using this combination of tools, we provide a set of mechanized proofs of the correctness and security properties of the protocol, or provide failed proofs and counterexamples if the protocol insufficiently fulfills the formalized domain models and requirements. Because the tools we choose are based upon automated solvers, proofs are implicit, as when solvers return successfully the properties that they are verifying

[9] See http://cryptol.net/, http://prosecco.gforge.inria.fr/personal/bblanche/proverif/, http://prosecco.gforge.inria.fr/personal/bblanche/cryptoverif/, and https://fstar-lang.org/. Other systems that can be used for this mechanization and reasoning and with which we are familiar include EasyCrypt, Tamarin, CPSA, and FCF. There are a few new tools available in the literature with which we have no familiarity, and that may be unavailable for commercial work, including SAPIC and ProScript. We are reaching out to our colleagues in the community about these tools.
[10] See http://saw.galois.com/
[11] See FlexTLS: A Tool for Testing TLS Implementations by Beurdouche et al. published in WOOT 2015.
[12] See http://frama-c.com/
[13] See http://www.openjml.org/

hold. There are alternative backend solvers that we can choose to use to generate explicit proofs if the Canton wishes to have such an artifacts.

We provide three kinds of proofs:

A. *A correctness proof of all correctness properties stipulated by the system requirements.* In the context of an E2E-VIV system, correctness proof components focus upon the properties stipulated by the requirements on the system. Essentially, all behavioral properties that are not security properties are correctness properties. The most common correctness properties in non-trivial algorithms focus on invariants of state machines, side conditions in proofs, etc.

B. *A symbolic security proof.* In this proof the cryptographic primitives are assumed to be perfect black boxes, modeled by axiomatically defined functions in an algebra of terms. Messages are terms on primitives, and a Dolev-Yao adversary model is used. We provide a symbolic security proof through the use of ProVerif and F*, both of which have built-in support for the verification of symbolic security properties.

C. *A computational security proof.* In this model, messages are bitstrings, cryptographic primitives are functions on bitstreams, and the adversary is any probabilistic Turing machine. This is the model supported by Cryptol and CryptoVerif, as well as via a detailed F* specification.

Note that we have chosen not to use a model-checking based specification and verification system because, in our experience, they do not scale well (in effort or capability) to protocols as rich as the chVote protocol.[14]

V. Consultancy.

We provide consultancy to the authorities on matters relating to the state-of-the-art in:
(a) building an assurance case for an implementation of the protocol;
(b) formal specification and reasoning about protocol, algorithms, and systems;
(c) rigorous engineering methods and tools, particularly those that are correct-by-construction for the trusted computing base of the chVote system;
(d) techniques through which expensive computations can be distributed in a secure, privacy-preserving fashion; and
(e) matters of usability and accessibility, especially in the context of E2E-VIV.

Project Management

Each project under execution at Free & Fair has a Scientific Leader who holds overall responsibility for the project. For this project, that leader is Dr. Joseph Kiniry. Each project also has a Project Leader (PL) who holds overall responsibility for project execution and client caretaking. For this project, that PL is Dr. Stephanie Singer.

[14] The technologies of this class that we use include UPPAAL, FDR, SAL, and Tamarin.

All other performers are grouped according to their roles and communicate and coordinate in a peer-to-peer fashion. The cryptographers we have available to potentially perform on this project include Dr. Alex Malozemoff, Mr. Tom DuBuisson, Mr. Ian Blumenfeld, and Dr. Gilles Barthe. The formal methods experts we have available to potentially perform on this project include Dr. Daniel Zimmerman, Dr. Joey Dodds, Dr. Robert Dockins, Mr. Trevor Elliott, Dr. David Cok, Dr. Aaron Tomb, Dr. Brian Huffman, Mr. Adam Foltzer, and Dr. Daniel Wagner. Each role has a Role Lead who coordinates performing.

For this project, our Role Lead for cryptography is likely Dr. Alex Malozemoff, and for formal methods is likely Dr. Daniel Zimmerman.

Biographies, CVs, publication lists, and more for all performers can be made available to the Canton on request. All are easily found via Google as well.

Free & Fair prefers to work on all projects in a public space under Open Source Initiative (OSI) or Creative Commons licensing.[15] Virtually all of Free & Fair's projects are hosted on GitHub in repositories.[16] Public project planning is executed using GitHub Issues and Milestones. OmniPlan from Omni Group is used for project management.[17] Google Docs is used for all shared documents, spreadsheets, and presentations. Google Hangouts is used for video chats within the team and with the client. Finally, polished reports which are literate documents are written in either Markdown or LaTeX.

Work Packages, Milestones, and Deliverables

Our proposed Work Packages mirror the Statement of Work above. Each Work Package has at least one Deliverable (labelled with a Deliverable number, such as **D1**), and our effort estimate for each Deliverable is reflected in its price (see the Budget section).

- **WP-DOM:** Domain Engineering
  - **D1:** Informal domain model of chVote in GSSL.
  - **D2:** Formal domain model of chVote in GSSL.
  - **D3:** Formal domain model of chVote in HOL.
- **WP-REQ:** Requirements Analysis
  - **D4:** Informal requirements in GSSL.
  - **D5:** Formal requirements in HOL.
- **WP-RISK:** Risk Assessment
  - **D6:** Threat identification in GSSL.
  - **D7:** Risk analysis report.
  - **D8:** Risk computation engine.

[15] See https://opensource.org/ and https://creativecommons.org/
[16] See https://github.com/FreeAndFair
[17] See https://www.omnigroup.com/omniplan

- **WP-PRIM:** Mechanized Primitives
  - **D9:** Cryptol specifications of all primitives used in chVote.
  - **D10:** Fully characterized symbolic stubs of primitives in protocol verification tools.
- **WP-PROTO:** Mechanized Protocol
  - **D11:** Protocol mechanized in Cryptol.
  - **D12:** Protocol mechanized in ProVerif.
  - **D13:** Protocol mechanized in CryptoVerif.
  - **D14:** Protocol mechanized in F*.
- **WP-CP:** Mechanized Correctness Proof
  - **D15:** Correctness proof.
- **WP-SSP:** Mechanized Symbolic Security Proof
  - **D16:** Symbolic security proof.
- **WP-CSP:** Mechanized Computational Security Proof
  - **D17:** Computational security proof.
- **WP-CONSULT:** Consultancy
  - **D18:** Final project report and presentation.

Figure 1 shows the dependencies among Work Packages. An arrow from one element to another indicates that the element at the source of the arrow is a dependency for the element at the head of the arrow. Consequently, artifacts earlier in a path must be completed prior to those later in a path. For example, artifacts in **WP-CP** cannot be started until those in **WP-PROTO** are complete.

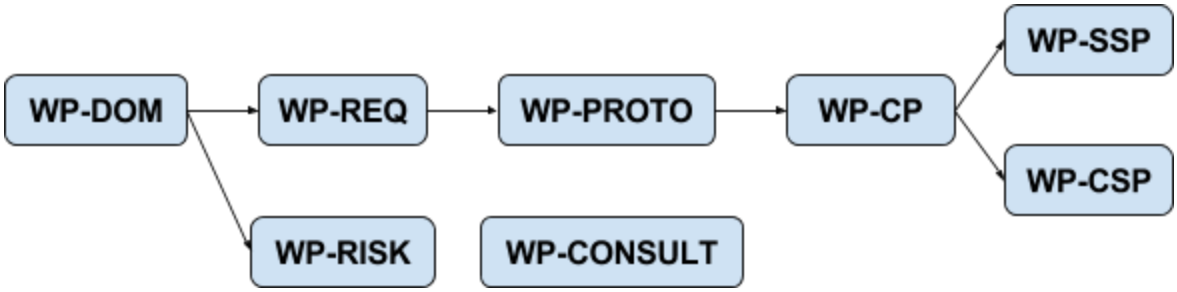

Figure 1: Work Package Dependencies

Project Risk Management

This project has an unusual framing insofar as the chVote protocol is not yet complete, polished, and published, has not seen external peer review from the community of cryptographers that work on end-to-end verifiable protocols, and does not yet have a draft informal security proof. As such, there is project risk in formalizing the protocol and attempting correctness and security proofs.

More specifically, any changes in protocol design can trigger potentially a significant amount of new work, including revising the protocol's core domain model (if new principles are introduced

or existing principles are changed), risk analysis (if the threat model of the protocol is changed), and mechanization (as any changes in protocol entail revisions in formalization).

If in the course of this project we find fundamental flaws in the chVote protocol, we will report each flaw, provide counter-example traces or incomplete proofs that precisely characterize the flaw, and offer ideas for suggested remedies. Any changes to our existing artifacts that are triggered by remediations of discovered flaws, or by changes to the protocol during project execution, will be billed at our hourly consulting rate.

Another risk inherent in this kind of work is critical performance unavailability. Our cryptographers and formal methods experts have a broad range of skills; most know many specification languages, at least one logical framework, and at least one formal method. Some of them have deep experience with the specific tools we propose using in this project (ProVerif, CryptoVerif, and F*), while others have deep experience in comparable tooling. If a specific performer with deep experience is unavailable at a given critical stage of the project, we will endeavor to put the highest efficiency adjacent expert on the task, even though doing so will likely result in a less efficient execution. In general, we will update the client regularly with respect to such task assignments and similar.

If in the course of this project we find that the existing verification technology is incapable of providing assurance artifacts (i.e., a given tool is incapable of finding a proof of a particular mechanized security property), we will offer alternative means by which to provide comparable assurance within the timeline and budget of the project. For example, a given security property may not be checkable using ProVerif, but may be checkable using F*.

Scheduling

Figure 2 is the Gantt chart for this project. Note that the scheduled end date of the project is 15 December 2017. Working backwards from that date we can estimate our latest start date as 24 April 2017 given current performer availability.

Free & Fair
http://freeandfair.us
421 SW 6th Ave., Suite 300
Portland, Oregon 97204
T 971.808.3247
F 503.350.0933

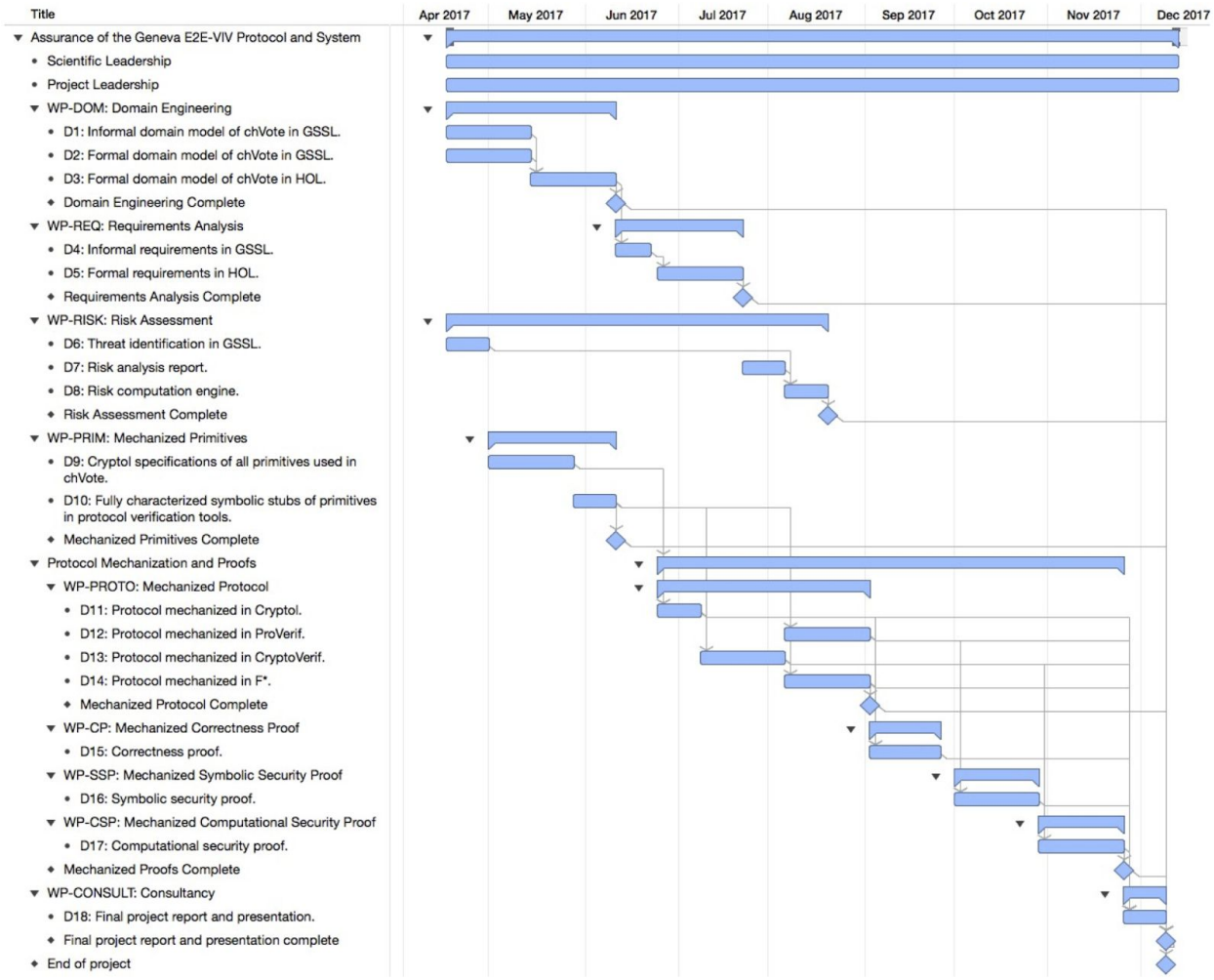

Figure 2: Project Gantt Chart

Budget

This project is budgeted by Deliverable. Consequently, the client can budget based upon a subset of work so long as dependencies are fulfilled. The following table contains a price for each Deliverable, as well as the total price for all Deliverables.

Task	Price
D1: Informal domain model of chVote in GSSL.	$53,000
D2: Formal domain model of chVote in GSSL.	$61,000
D3: Formal domain model of chVote in HOL.	$61,000
D4: Informal requirements in GSSL.	$30,000
D5: Formal requirements in HOL.	$61,000
D6: Threat identification in GSSL.	$26,000
D7: Risk analysis report.	$30,000
D8: Risk computation engine.	$27,000
D9: Cryptol specifications of all primitives used in chVote.	$52,000
D10: Fully characterized symbolic stubs of primitives in protocol verification tools.	$26,000
D11: Protocol mechanized in Cryptol.	$26,000
D12: Protocol mechanized in ProVerif.	$60,000
D13: Protocol mechanized in CryptoVerif.	$52,000
D14: Protocol mechanized in F*.	$52,000
D15: Correctness proof.	$55,000
D16: Symbolic security proof.	$57,000
D17: Computational security proof.	$57,000
D18: Final project report and presentation.	$26,000
Total Price	$812,000

Table 1: Project Budget

Consultancy as a part of Work Package **WP-CONSULT** is billed in 30 minute intervals at a rate of US$350/hr.

Other Statements Material to this RFI

Nothing in this response is proprietary or secret. Free & Fair publishes all of its RFI and RFP responses for government agencies, all proposals we write for Foundations and research funding agencies, and all artifacts relevant to our open source, rigorously engineered, high assurance elections systems. As such, unless the Canton of Geneva wishes otherwise, we will publish this response in the coming weeks.

Conclusion

We are happy to answer any other questions the Canton of Geneva might have about our products and services. The Canton is treating the assurance of its digital elections technology seriously, as befits such a critical component of the democratic process, and we look forward to helping the Canton achieve the assurance goals mandated by the PoRA, PoRO, VEleS, and Annex.

Free & Fair
http://freeandfair.us
421 SW 6th Ave., Suite 300
Portland, Oregon 97204
T 971.808.3247
F 503.350.0933