Secure Document Transfer System for Military and Overseas Voters

RFI #2016000004
Colorado Department of State
22 September 2015

Dr. Joseph R. Kiniry, Galois, Inc., kiniry@galois.com
Dr. Daniel M. Zimmerman, Galois, Inc., dmz@galois.com

Responder

Galois, Inc., 421 SW Sixth Avenue, Suite 300, Portland, OR 97204

Point of Contact

Jodee LeRoux, Contracts
Galois, Inc.
421 SW Sixth Avenue, Suite 300
Portland, OR 97204
ph 503.808.7209
contracts@galois.com

Company Overview

Galois is a privately held U.S.-owned and -operated company established in 1999. Our mission is to provide trustworthiness in critical systems. We were founded on core principles that focus on innovation, authenticity, and deep trust, and we live those principles every day in interactions with clients and among ourselves. We specialize in the research and development of new technologies that solve the most difficult problems in computer science. Our team works closely with clients to achieve a balance among the privacy/cost/speed challenges involved in making systems more trustworthy.

Galois has 60 employees in 2 offices (Portland, Oregon and Arlington, Virginia), with principal investigators leading research and engineering teams in the areas of cryptography, software correctness, mobile security, cyber physical systems, computer security, machine learning, human machine interaction, and scientific computing. We have won and successfully executed on dozens of multi-year, multi-million dollar R&D projects for numerous federal agencies including the Department of Defense (DOD), the Department of Homeland Security (DHS), Defense Advanced Research Projects Agency (DARPA), Department of Energy (DOE), NASA, and members of the Intelligence Community.

Galois has a fifteen-year proven track record of solving the most complex challenges of the most demanding federal and commercial customers. Our bespoke software products are internationally recognized as being some of the best technology in the world of high-assurance software systems. Consequently, we intend to fundamentally change the nature of elections systems design, development, and support and put the power back in the hands of the voting public.

Early in Galois's existence we recognized that democracy should be treated as a high-assurance system, so we have had a long-term interest in developing technology for elections. A high-assurance system, or trustworthy system, is a system 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 historically 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).

Historically, Galois has not executed on election systems. However, we have successfully developed many systems that have many of the same challenges (correctness, security, usability, accessibility, etc.) and technologies (operating systems, programming languages, distributed systems, cryptography, etc.). Thus, we are well positioned to bring the assurance one sees in other safety- and mission-critical high-assurance systems to the elections systems and services market, at low cost and with publicly owned open source technology on COTS hardware.

Galois has a flat, peer-to-peer organizational structure. Senior personnel who have national or international experience relevant to the development of elections systems include Dr. Joseph Kiniry (an internationally recognized expert in high-assurance systems, security, and elections), Harri Hursti (an international elections security expert, who has been infamously involved in several state-mandated deep audits of elections technology), Maggie MacAlpine (a national election processes and auditing expert), and Dr. Daniel Zimmerman (a former professor at two institutions and an internationally recognized expert in high-assurance systems design and development).

For the past year, we have been developing prototype technologies in this space that include an electronic poll book, a verifiable in-person voting system, and tabulation and auditing techniques that support ranked choice voting. We are in the process of spinning out a class B corporation, Verifiable Elections, whose mission is to bring open source, high-assurance, end-to-end verifiable elections to the world. This new company will be a Galois-branded entity and will retain much of the personality, history, technology, and performers of Galois. Dr. Kiniry is the Chief Scientist and CEO of Verifiable Elections, and Dr. Zimmerman is a key member of its management team.

Prior to working for Galois, Dr. Kiniry provided commercial and public consultancy services to several governments on matters relating to elections, their technology, security, processes, and verifiability. His experience in the area of elections is both from the perspective of a public employee (as he was a professor of computer science and mathematics at multiple universities for approximately twelve years) and as a scientist-activist. He has worked on election systems for thirteen years; has audited the security, correctness, and reliability of numerous physical and internet-based voting systems; has developed high-assurance prototypes and products of several election technologies (including, but not limited to, tallying, auditing, voting, ballot marking, and electronic poll book systems); and sits on the Board of Advisors of the main verifiable elections nonprofit, Verified Voting.

Dr. Kiniry has formally advised three governments (The Netherlands, the Republic of Ireland, and Denmark) on matters relating to digital elections and has testified before two parliaments. He has also provided informal input and advice to the governments of Norway, Estonia, and the U.S.A. He co-ran a multi-year research project on digital elections (the DemTech project) and has supervised numerous BSc, MSc, and PhD theses focusing on elections technologies. His research group has developed several high-assurance peer-reviewed election software systems, including a tally system used in binding European elections for The Netherlands and an electronic poll book system meant to be used in Danish national elections.

Dr. Kiniry also regularly interacts with and provides input to federal agencies related to elections including the EAC, NIST, and FVAP, and several elections-related non-profits including the OSET Foundation, Common Cause, Democracy Works, the Overseas Vote Foundation, and U.S. Vote. Dr. Kiniry is a key actor in the newly formed NIST-EAC Public Working Groups.

Dr. Zimmerman, the Technology Lead at Verifiable Elections, has extensive experience in formal methods, high-assurance software engineering, concurrent and distributed systems, and foundations of computer science. Before coming to Galois, he taught computer science at multiple universities for over a decade. At Galois, he has worked primarily in the areas of rigorous software engineering and verifiable elections technology.

Harri Hursti has focused on uncovering data security problems in electronic voting systems globally. He has revealed severe problems in electronic voting systems worldwide, and is famously known for developing the Hursti Hack, in which he demonstrated how the voting results produced by the Diebold Election Systems, Inc. voting machines could be altered. The Hursti Hack was verified by scientists from UC Berkeley, commissioned by California's Secretary of State. HBO turned the Hursti Hack into a documentary called "Hacking Democracy", which was nominated for an Emmy award for outstanding investigative journalism. He has subsequently been involved with various academic studies on elections, including the EVEREST study commissioned by Secretary of State of Ohio.

Margaret MacAlpine, Auditing Specialist at Verifiable Elections, has managed risk limiting and transitive audits in Florida, Connecticut, and most recently in Colorado. She has served as an advisor of the office of the Secretary of State of California for the Risk Limiting Audit Pilot Program 2011-2012, and is widely regarded as an expert on the use of high-speed scanners for conducting election audits. She also contributed to the “Security Analysis of the Estonian Internet Voting System”[1] in partnership with the University of Michigan.

[1] https://estoniaevoting.org/findings/paper/

Galois is uniquely positioned to respond to an RFP from Colorado based upon this RFI because we were the technical lead on the U.S. Vote Foundation's End-to-End Verifiable Internet Voting (E2E-VIV) project,[2] a two year project whose entire focus was on the requirements stipulated in this RFI to address the needs of UOCAVA, overseas military, and disabled voters. Dr. Kiniry and Dr. Zimmerman are the coauthors of the resulting E2E-VIV report, discussed later in this response. As such, we are the premier organization worldwide to address the concerns of the Colorado Secretary of State on these matters.

In general, Galois's work, reputation, and way of doing business—based upon trustworthiness, authenticity, and transparency—means that virtually all our customers become repeat customers. Consequently, we are happy to introduce any potential client to any existing or past client as a referral.

Reflections on the Proposed System

The Colorado Department of State, in order to ensure that military and overseas Colorado voters are able to participate in Colorado elections, has deployed a system for electronically delivering ballots to those voters. This RFI was issued to determine the feasibility of deploying a system that would complement the existing ballot distribution system by allowing military and overseas Colorado voters to securely return their voted ballots to their county clerks and recorders.

Since the documents to be securely transferred are voted ballots, such a secure document transfer system would constitute an Internet voting system. Implementing a secure Internet voting system in general is very challenging, because the architecture of the Internet is not amenable to ensuring the security, integrity, and privacy requirements of voting: malware on voters' computers may prevent voters from submitting their ballots or change submitted ballots so they no longer reflect voter intent; denial-of-service (DoS) attacks may prevent delivery of blank ballots to voters, prevent delivery of voted ballots to election officials, or overwhelm election systems with invalid data on Election Day; and election systems must ensure that only registered voters can vote, in an environment where personally identifying information stored in the databases of organizations ranging from Sony Corporation to the U.S. Office of Personnel Management has been repeatedly compromised.

In order to be trusted by both voters and election officials, an Internet voting system must provide some assurance that it is correctly recording voter intent. One type of assurance is called *end-to-end verifiability* (E2E-V), and an Internet voting system that provides it is called an *end-to-end verifiable Internet voting* (E2E-VIV) system. In an E2E-VIV system, the result of the election process matches the intentions of the voters: each voter is assured that her vote is cast as intended, recorded as cast, and counted as recorded.

The present RFI asks for a system that allows military and overseas voters to return ballots in a secure, private, easy, and accessible manner. These are overly broad and underspecified requirements. If they are interpreted in the manner that we describe in *The Future of Voting:*

[2] https://www.usvotefoundation.org/E2E-VIV

End-to-End Verifiable Internet Voting – Specification and Feasibility Assessment Study,[3] the current state-of-the-art in cryptography and Internet application technology is insufficient to build an E2E-VIV system that completely satisfies all of them. Reconciling the privacy and security requirements is particularly problematic. However, since the goal for the desired submission system is to provide a method solely for overseas and military voters to return their ballots, we can create a secure, easy-to-use, accessible system if CDOS permits some flexibility with respect to voter privacy.

Currently, under C.R.S. 1-8.3-113, Colorado voters are permitted to return their voted ballots by electronic means "in circumstances where another more secure method, such as returning the ballot by mail, is not available or feasible, as specified in rules promulgated by the secretary of state." Under the Colorado Secretary of State rules for such circumstances adopted in August 2015, a voter must submit an affirmation that includes the language, "I also understand that by returning my voted ballot by electronic transmission, I am voluntarily waiving my right to a secret ballot and that Colorado law requires that I return this ballot by a more secure method, such as mail, if available and feasible." With this affirmation, military and overseas voters who return their ballots electronically waive their ballot secrecy rights as a matter of course. Their votes are disclosed to—at minimum—the recipient of the email or fax transmission containing the ballot, the bipartisan team of election judges assigned to duplicate the ballot, and the appropriate county clerk.

Galois's Recommendation

If CDOS is willing to permit UOCAVA and military voters in extraordinary situations to continue to waive their privacy to submit their votes digitally under C.R.S. 1-8.3-113, then we have a proposed technical solution for Colorado.

In short, our system design fulfills all of the requirements (1–21) stipulated in the RFI and enables a voting process that looks and feels similar to performing a direct deposit of a check from a mobile phone. The resulting digitally-submitted ballots are the official ballots for tabulation purposes. We also recommend that, whenever possible, voters also physically mail their signed ballots to their county clerks. Having a subset of the signed paper ballots—even if they arrive late—facilitates post-election risk-limiting audits for election verification, which can provide objective evidence that the digital procedures used to submit extraordinary UOCAVA and military voters' ballots have not impacted the overall election outcome.

In particular, in our system:

A. Voters receive authentication credentials with digital blank ballots.

B. Offline ballot marking (e.g., using a browser or a PDF previewer) is supported, but not mandatory. Physically printing and filling out paper ballots by hand is preferred.

[3] https://www.usvotefoundation.org/e2e-viv/summary

C. Voters must physically sign the completed printed ballot so that traditional signature matching for voter authentication is still possible.

D. A smartphone app is used to perform a "direct deposit" of the photographed ballot. We can easily support Apple and Android devices. If there is a mandatory requirement for other mobile operating systems or support for desktop/laptop computers, this can be addressed, though it has greater cost and usability challenges.

E. The signed, photographed ballot is digitally signed and encrypted prior to transport by the mobile phone app.

F. The app performs end-to-end secure transport directly to a cryptographically secure data store.

G. The voter receives a cryptographic receipt when their ballot is received by the secure data store, and another receipt when their LEO downloads their ballot from the data store.

H. LEOs can authenticate to the data store and download ballots destined for them in a quick and easy fashion with any web browser.

I. Various kinds of multi-factor authentication are available to LEOs. We recommend Tozny[4] or Yubikey,[5] both of which leverage physical tokens and are low cost.

J. The secure data store can be either an on-premises server or hosted in one of several cloud data store providers, as appropriate to satisfy state data retention policies. We recommend using a cloud service, since doing so can lower cost and increase assurance and availability.

As with all of our offerings, our solution will be designed and constructed using the concepts, tools, and technologies we use at Galois for safety- and mission-critical products and services for our existing clients.

We recommend that the entire system be formally specified, all protocols be formally verified for both correctness and security properties, and that the entire system be designed, built, validated, and verified using our rigorous engineering methodology.

Finally, we strongly suggest that the entire system, including all engineering artifacts such as requirements documents, designs, architecture specifications, source code and its documentation, low-level formal specifications, and evidence of correctness, be made available to the public under a liberal Open Source Initiative (OSI) license.

In the following section we provide more detail about our technical capabilities and these recommendations.

[4] http://tozny.com/

[5] https://www.yubico.com/

Galois Verifiable Elections R&D

Our design and architecture for election-related systems is highly modular. Each module uses only open data formats for communication, resulting in a system that can be modified and upgraded by anyone who is familiar with the open standards that we use. This modular architecture features an air gap between the software responsible for running the election and the software for designing and reporting on it. A modular architecture assists with compositional validation and verification, experimentation with user experience variants, and phased user acceptance testing. It can also ease customization of the system, allowing new voting methods and ballot styles to be swapped into the system as needed without requiring system-wide changes. Modular design also aligns with what we expect to see in version 2.0 of the U.S. Election Assistance Commission's Voluntary Voting System Guidelines.

Our cryptographic foundations, ranging from authentication to data-at-rest to provenance-preserving logging, are based upon our work on another one of our products, Cryptol,[6] and a host of advanced tools and technologies for ourselves and academic partners. In general, our systems use cryptographically secure authentication and credentials issuance (via technologies like multi-factor authentication), cryptographic databases, cryptographic hardware (including FIPS-certified libraries and hardware), custom formal protocol design and verification, custom formally verified cryptographic libraries, and logging with privacy-preserving cryptographic integrity.

Our systems are all fault tolerant and have sufficient redundancy, both in algorithm design and physical architecture, to ensure that they can survive the simultaneous failure of multiple machines or networks.

Software correctness is an integral part of the Galois development approach, beginning with the specification of a system's domain model, requirements, and software and network architecture. By formally specifying the initial design, and developing the implementation based on the resulting specification, we guarantee that we are implementing exactly the desired system. We also incorporate the vast majority (typically on the order of 99%) of the software tests within the code itself, rather than developing tests separately, and these tests are, for the most part, generated automatically from formal specifications. This leads to a software product built with quality inherent in its foundation, rather than with defects to be detected and fixed later. In addition to this pervasive testing, quality assurance is achieved through strict configuration management and systematic validation of the code as well as the all evidence-based artifacts and documentation produced.

For the most essential parts of the software we go a step further, performing a machine-checked functional verification of the software. In this process we first design a mathematical model that should be as easily understood as the English language specification. We then provide an implementation that is mathematically proven to meet the specification. This mathematical proof can be automatically checked on any computer, giving unparalleled assurance that the software is correct. These techniques have historically been used for safety-critical systems, where the

[6] http://www.cryptol.net/

failure of a system would result in loss of life (e.g., flight control systems at Airbus) or have enormous cost implications (e.g., failure of a mission to Mars).

By combining these approaches, we get a chain of correctness that starts with the high-level system specification and continues all the way down to the smallest implementation details of the most critical parts of the system. At each step in the chain we focus on providing evidence of correctness, generally in multiple forms, including for example refinement proofs from informal to formal specifications, unit test suites, and mathematical proofs of correctness and security. In other words, all the effort we put into ensuring that our system is correct generates tangible artifacts that give external parties the same confidence in our software that we have.

The specific peer-reviewed methodology we use for all of our software is a variant of Design by Contract[7] with some aspects of a Correctness by Construction[8] approach. Our process, method, tools and technologies span several deployment and development platforms, specification and programming languages, and communication and coordination schemes.

Support, Staffing, and Help Desk Services

Galois recognizes that any system implementation not only requires a technically sound and robust product with comprehensive business functionality at its core, but also needs to be supported by professional services throughout the project life cycle. We have expertise in professional services such as project/program management, software design and development, testing, mentoring and training, implementation and go-live as well as post-implementation operational support services.

At Galois, we typically run a very lean ship when it comes to project management and customer caretaking. We can be lean because our research engineers are all 10x programmers, most of whom have PhDs, and because of our focus on trust and transparency in all business and technology.

For example, we use a model for service guarantees and operational support that is atypical because our systems are high-assurance and formally verified. Instead of a traditional triaged tiered support system, we provide a comprehensive support solution that emphasizes transparency about the product and its capabilities and direct access to the team responsible for the product.

For our traditional projects, customers have direct telephone and email access to the project lead, direct access to the project's ticket system, and direct visibility into the development repository of the project. Support tickets filed in the system are typically triaged by team members within minutes, responses to issues are immediate, and fixes are prioritized based on conversations between the customer and the development team. We can provide evidence of these claims by simply referring evaluators to our Open Source product repositories.

[7] https://en.wikipedia.org/wiki/Design_by_contract
[8] https://buildsecurityin.us-cert.gov/articles/knowledge/sdlc-process/correctness-by-construction

For field support during deployment and system use, we augment operational support with a front-line team that can provide basic support to election officials and volunteers. We plan to provide support of this kind via a toll-free number, an online text chat interface, online video chat support, or any combination of these.

We also provide training offerings related to our products; Open Source technology adoption, legality, and use; certifications; evolving national and international standards in elections technologies; and rigorous software development.

Despite the fact that our products are high-assurance and include a wide range of untraditional artifacts—such as formal specifications, tests, and proofs—to guarantee their correctness, security, usability, and accessibility, they are no more expensive than existing products. In fact, our methodology is intended to significantly decrease the cost and time of certification.

Targeting the November 2016 Election

Based on the time constraints laid out in this RFI, with the goal of full deployment for the November 2016 election and the anticipated release of the RFP in early 2016, we recommend that development of the proposed system be completed no later than June 2016. We also recommend conducting mock elections (at least one if not two cycles) in addition to user and system acceptance testing to ensure that the system is ready for the demands of a live election in a presidential election year. The mock elections should be conducted over a good representative sample of voters to cover variances in ballot size and complexity, multilingual ballots, accessibility needs, and other critical aspects of the voting process.

Conclusion

Please feel free to get in touch with us if you have any questions or comments. We look forward to seeing an RFP from Colorado on these topics and hope that our input has been useful.