End-to-End (E2E) Verifiable Protocols for Voting Systems

Andy Regenscheid – Voting Security Team, NIST
Principle 9: AUDITABLE
The voting system is auditable and enables evidence-based elections.

• Two paths for software independence (9.1.1-A):
  • Paper-based System architectures
  • E2E Verifiable System Architectures
• E2E Systems must use approved cryptographic protocols (9.1.6-A)
• E2E Systems must undergo an independent evaluation of its implementation of an approved protocol (9.1.6-B)

Goal: Establishing a public process to solicit, evaluate, and approve E2E verifiable voting protocols that could be implemented in voting systems.
What is E2E Verifiability?

Vote Marking  Casting  Counting

Voter Verifiability: Voters can check their ballot was correctly cast/recorded

Universal Verifiability: Anyone can verify cast ballots were correctly counted
Raising Hands in a Group: Verifiable, but not private
E2E-V Properties

- Cryptographically auditable voting protocols
  - \textit{Cast as Intended}: Voters have confidence that their cast vote selections reflect intent
  - \textit{Recorded as Cast}: Voters can confirm their cast ballot was included in the results
  - \textit{Tallied as Recorded}: Vote counts are publicly verifiable

- Software Independent by design
  - \textit{Paper-Based Systems}: Auditability achieved through voter-verifiable paper records and election procedures
  - \textit{E2E Systems}: Auditability achieved through mathematical proofs; may also use paper records

- E2E protocols must provide these properties while also supporting usability, accessibility, security, privacy and functional requirements
What is E2E Verifiability?

Vote Marking → Casting → Counting

Cast as Intended
What is E2E Verifiability?

Vote Marking → Casting → Counting

Recorded as Cast

Tallied As Recorded

Jan. 26, 2023
TGDC Meeting
Evaluation Challenges

• **Lack of Standards**
  • E2E protocols are application-specific
  • Use non-standard cryptographic algorithms

• **Security Analysis**
  • Protocol and algorithm evaluations require careful review by subject matter experts

• **Accessibility**
  • New voter verification/auditing processes present unique accessibility challenges

• **Testing Implementation in Voting Systems**
  • Systems must properly implement protocols to be software independent
  • Protocols must be securely implemented to avoid errors and preserve ballot secrecy
E2E-V Workshop

The Path to E2E Verifiable Protocols for Voting Systems

Purpose: Bring stakeholders together to begin the process of:

• Building a community of interest
• Identifying what is needed from E2E verifiable voting protocols and systems
• Establishing a public evaluation process for protocols
• Discussing requirements and evaluation criteria for a call for proposals

Oct. 6-7, 2022
Agenda

Opening Remarks: Chairman Hicks, EAC
Keynote- E2E Verifiability- Ben Adida, VotingWorks
Overview Of E2E Eval. Process- Andy Regenscheid, NIST
Panel 1: Integrity and Voter Confidence
Panel 2: Security
Panel 3: Accessibility and Human Factors
Panel 4: Implementation and Testing
Next Steps- Jon Panek, EAC
Closing Remarks: Chairman Hicks, EAC
E2E-V Workshop Feedback

• **E2E-V Voting Systems have unique and valuable characteristics**
  - Improve voter confidence/trust
  - Facilitate development of new voting system architectures

• **Significant challenges remain**
  - Complexity may reduce voter acceptance and trust – communication will be key
  - Technical evaluation of protocols and systems is difficult
  - Accessibility of voting and verification methods is critical

• **Move deliberately and thoughtfully**
  - “Nothing erodes trust more than getting it wrong with voter”

• **Open and transparent processes are critical**
  - Involve a diverse group of stakeholders
  - Allow public to see, analyze, and contribute to the process, provide open documentation

• **Learn through incremental progress**
  - Consider encouraging/facilitating pilot projects to learn from real-world systems
Takeaways

- More research and community engagement is needed before initiating a call for proposals

- Protocols and system designs continue to change to support new properties and features, e.g.,
  - Support different voting variations
  - Back-end optimizations
  - Quantum resistance

- Stability needed to make evaluation/certification practical and cost-effective
  - E2E verified voting protocol evaluation
  - Protocol implementation evaluation
  - System-level certification

- NIST continues to believe an open and public process should be used to evaluate protocols

Previously-Proposed Plan

- **Community Building**
  - Detail the plan - process, scope, etc.
  - Establish public feedback mechanisms

- **Call for Proposals**
  - Draft and seek input on evaluation criteria
  - Release CFP to formally initiate process

- **Evaluation (Multiple Rounds)**
  - Publish complete submissions publicly
  - Engage stakeholders in public events

- **Selection Decisions**
  - Analyze public feedback and make selections
  - Publish decision rationale

- **Maintenance**
  - Maintain specifications for protocols
  - Review any new research/findings

- **Testing and Certification**
  - Determine testing and evaluation methods for E2E protocol implementations
Needed Research Areas

• Accessibility and usability of E2E verifiable voting systems
  • For voters, pollworkers, and election officials using these systems
  • Address full process – system setup, voting, verification, and auditing

• Impact on election management and pollworker responsibilities
  • E2E verifiable voting systems introduce new steps to the process
  • New system components, e.g., verification website

• Public transparency and trust in E2E verifiable voting protocols
  • Study perceptions and trust in E2E verified voting protocols and systems
  • Communicating E2E verifiability to the public/voters

• New methods/designs for E2E verifiable voting systems
  • Front-end: Different protocols/designs to support different interfaces and voter interaction
  • Back-end: New cryptographic protocol/designs to support voting variations and quantum resistance

• Use of E2E verifiable protocols as an incremental tool
  • Consider different usage scenarios where E2E verifiability could add to the voting process
Questions

• Are there other research areas or questions that NIST and the EAC should investigate?

• How can NIST and the EAC facilitate incremental progress in E2E verifiable systems?
  • What pilot projects or studies could be done?
  • How could/should we address usage of E2E verifiable voting protocols in otherwise software independent systems?

• How and where can we bring the election officials, technologists, manufacturers, and advocates together to discuss challenges, needs, and solutions?

Jan. 26, 2023

TGDC Meeting
Background: *Crypto Standards Processes*

- NIST has been developing cryptographic standards since the Data Encryption Standard in the 1970s
- Similar challenges to vetting E2E protocols:
  - Difficult, multi-layered security evaluation process
  - Need to build confidence and trust to facilitate adoption
- Public evaluation processes valuing openness and transparency
  - Establish a community of interest with researchers, industry and practitioners
  - Develop open Calls for Proposals with clear requirements and evaluation criteria
  - Submissions open for public view, typically over multiple rounds
  - Rationale for decisions are publicly documented
Example: PQC Selection Process

Community Building
- Foundational research
- Workshops
- Participation in academic events

First Round
- 82 Submissions Received
- 69 accepted as complete and proper

Second Round
- 26 candidates selected for Round 2
- Rationale published in NISTIR 8240
- 2nd PQC Conference

Public Evaluation
- 3rd PQC Conference
- Analysis of research results

(Call for Proposals)
- Public comments on requirements and evaluation criteria
- Formal Call for Submissions

(2016)

(2017)

First Round
- 82 Submissions Received
- 69 accepted as complete and proper

Public Evaluation
- 1st PQC Conference
- Ongoing communication with researcher

(2018)

Second Round
- 26 candidates selected for Round 2
- Rationale published in NISTIR 8240
- 2nd PQC Conference

(2019)

Third Round
- 7 finalists and 8 alternates selected for Round 3
- Rationale published in NISTIR 8309

(2020)

Standards
- Initial selections announced
- Drafting standards

(2021)

2022
Previously-Proposed Process

- **Community Building**
  - Detail the plan - timeline, process, scope, etc.
  - Establish public feedback mechanisms

- **Call for Proposals**
  - Draft and seek input on E2E protocol requirements and evaluation criteria
  - Release CFP to formally initiate process, allowing new submissions annually

- **Public Evaluation (Multiple Rounds)**
  - Publish complete and proper submissions publicly
  - Engage stakeholders in public workshops, conference and online mediums

- **Selection Decisions**
  - Analyze public feedback and make selection decisions - Approve, Reject, Defer
  - Publish decision rationale

- **Maintenance**
  - Maintain open specifications for approved protocols
  - Review any new research/findings on approved protocols

- **Integration into Testing and Certification Program**
  - Determine testing and evaluation methods for E2E protocol implementations

TGDC Meeting 17 Jan. 26, 2023
What is E2E Verifiability?

Vote Marking

Casting

Counting

Jan. 26, 2023  TGDC Meeting