E2E Protocol Approval Process

Andrew Regenscheid, NIST
andrew.regenscheid@nist.gov

Agenda

- E2E Verifiable Voting Systems Overview
- E2E Protocol Approval Process
  - NIST Competition Reference
  - Proposed Process
  - Timelines for Process

E2E in the VVSG 2.0

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)

E2E Verifiable Voting Systems

- Cryptographically auditable voting protocols [1]
  - ***Cast as Intended***: Voters have confidence that the their cast vote selections reflect their intent
  - ***Recorded as Cast***: Voters can confirm their cast ballot was included in the results
  - ***Tallied as Recorded***: Vote founds are publicly verifiable
- Software Independent by design [2]
  - *Paper-Based Systems*: Auditability achieved through voter-verifiable paper records and election procedures
  - *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

E2E- Example

- **Casting:**
  - Makes selections on an electronic ballot marking device
  - Receive a confirmation code- an encrypted form of the selections
  - Verification process ensures the selections and confirmation code reflect intent
- **Record Verification:**
  - All encrypted votes are posted publicly
  - Voter can verify selections were included by matching confirmation code
- **Vote Counting:**
  - The system produces a verifiable mathematical proof that the vote tallies match the publicly-posted encrypted votes
    - e.g., the encrypted votes are combined and then decrypted to obtain the tally

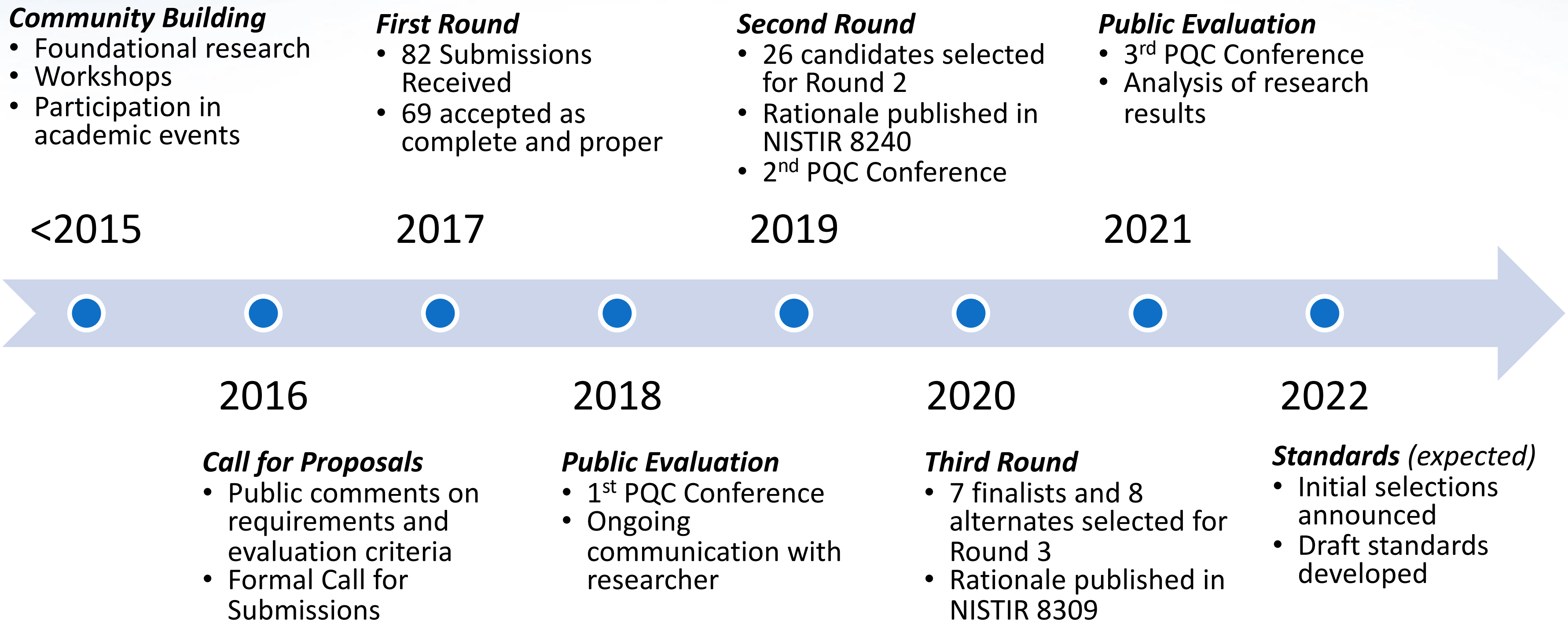
E2E Challenges

- **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
- **Usability/Accessibility**
  - New voter verification/auditing processes present unique usability/accessibility challenges [3]
- **Testing Implementation in Voting Systems**
  - Systems must properly implement protocols to be software independent
  - Protocol implementations must be secure to avoid leaking data and reliability

Background: *Cryptographic Standards Processes*

- NIST has been developing cryptographic standards since the Data Encryption Standard in the 1970s [4]
- 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*



<2015

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

2016

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

2017

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

2018

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

2019

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

2020

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

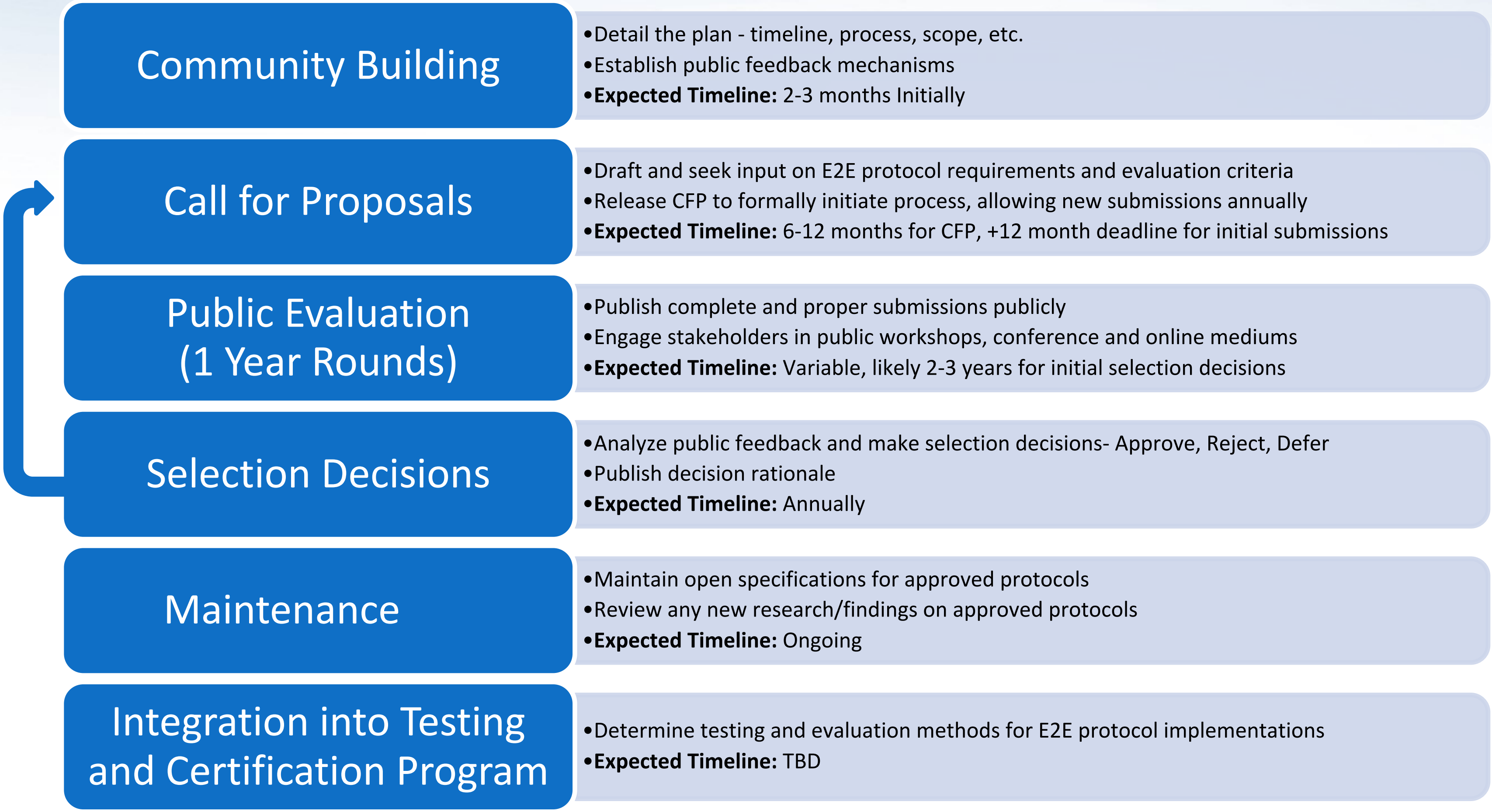
2021

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

2022

Standards *(expected)*
- Initial selections announced
- Draft standards developed

Proposed E2E Protocol Process



Community Building

- •Detail the plan - timeline, process, scope, etc.
- •Establish public feedback mechanisms
- •**Expected Timeline:** 2-3 months Initially

Call for Proposals

- •Draft and seek input on E2E protocol requirements and evaluation criteria
- •Release CFP to formally initiate process, allowing new submissions annually
- •**Expected Timeline:** 6-12 months for CFP, +12 month deadline for initial submissions

Public Evaluation (1 Year Rounds)

- •Publish complete and proper submissions publicly
- •Engage stakeholders in public workshops, conference and online mediums
- •**Expected Timeline:** Variable, likely 2-3 years for initial selection decisions

Selection Decisions

- •Analyze public feedback and make selection decisions- Approve, Reject, Defer
- •Publish decision rationale
- •**Expected Timeline:** Annually

Maintenance

- •Maintain open specifications for approved protocols
- •Review any new research/findings on approved protocols
- •**Expected Timeline:** Ongoing

Integration into Testing and Certification Program

- •Determine testing and evaluation methods for E2E protocol implementations
- •**Expected Timeline:** TBD

Community Building

- **Broad stakeholder engagement is critical**
  - Election officials
  - Cryptography and security researchers
  - Usability/Accessibility experts
  - Manufacturers and implementers
  - Advocacy and non-governmental organizations
- **Seek input**
  - Engage stakeholders where they are— existing organizations, conferences and events
  - Pull stakeholders into the E2E evaluation process
- **Build consensus**
  - Intended scope, process, and timeline
  - Critical objectives, requirements, and evaluation criteria
  - Engagement mechanisms

Call for Proposals

- **Submission Requirements**
  - Protocol specification and description of use
  - Security analysis and other supporting documentation
  - Reference implementations
  - Intellectual property disclosures/statements
- **E2E Protocol Requirements**
  - Auditability
  - Security
  - Human Factors
- **Evaluation Criteria**
  - Auditability and security properties
  - Maturity of design and supporting analysis
  - Usability/accessibility for voters, poll workers and election officials
  - Advantages over existing approved methods

Open call- submission accepted on an annual basis

Public Evaluation

- **E2E Submission Packages**
  - Publicly posted with reference implementations
  - Licenses facilitating research and evaluation
- **Public Engagement Methods**
  - Public mailing list(s)
  - Formal comments
  - Community Events/Conferences/Workshops
- **EAC/NIST Roles**
  - Provide venues/opportunities for public input
  - Actively engage relevant stakeholders
  - Technical evaluation of submissions and public feedback
  - Impartial authority assessing submissions

Selection Decisions and Maintenance

- Annual selection decisions of active submissions based on public evaluation:
  - **Approve:** Sufficient evidence that a submission meets requirements and evaluation criteria
  - **Reject:** Failure to provide sufficient evidence
  - **Defer:** Additional technical evaluation is needed to make a decision
- Multiple rounds of evaluation typically needed prior to making selection decisions
- Protocol specifications of approved submissions formally adopted in collaboration with submission team
  - Adopted specifications will need continuous review of any new results
  - Revisions addressed through public processes

Discussion Questions

- **Stakeholder Engagement**
  - How can we bring together election officials, manufacturers, and usability experts into this process?
  - What organizations, venues and events should be included?
- **Public Confidence**
  - How can we build public confidence in these types of complex voting systems?
- **Sustainability**
  - What is the right balance between maintainability and flexibility with the number and set of approved protocols?
  - How will cryptographic migrations and protocols updates be handled?
- **Testing**
  - What changes will be necessary to the Testing and Certification program?

Questions?

Andrew Regenscheid, NIST
andrew.regenscheid@nist.gov

References

1. Benaloh et al, *End-to-end verifiability*, 2015. https://arxiv.org/pdf/1504.03778.pdf
2. Rivest, Wack, *On the Notion of Software-Independence*, 2008. https://people.csail.mit.edu/rivest/RivestWack-OnTheNotionOfSoftwareIndependenceInVotingSystems.pdf
3. Acemyan, C. Z., Kortum, P., Byrne, M. D., & Wallach, D. S. (2015). From error to error: Why voters could not cast a ballot and verify their vote with Helios, Prêt à Voter, and Scantegrity II. Journal of Election Technology and Systems, 3, 1–25.
4. National Institute of Standards and Technology, *NIST Cryptographic Standards Development Process*, NISTIR 7977, 2016 https://doi.org/10.6028/NIST.IR.7977
5. NIST, *Post-Quantum Cryptography Standardization* https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization