



<http://www.oasis-open.org>

March, 2005



# Trusted Digital Ballot Processing in a Nutshell

Submission to OASIS EML TC  
by David RR Webber  
Chair OASIS CAM TC  
(True Vote Maryland member)

<http://drrw.net>

# Nutshell Overview

- This is for those who are in a hurry and just want to know the core principles contained in the trusted method
- Focused on just United States polling process today
- For the full reasoning and extended analysis supporting the process – see the main presentation –

<http://drrw.net/backup/Trusted-Ballot-Processing-Systems.pdf>

# Creating an open marketplace

- Trusted process that underpins voting in the digital age
- A healthy and open marketplace where a broad range of service providers can deliver solutions to citizens, using off-the-shelf cost-effective components, that support and enhance the voting system and experience
- Based on open specifications that have free use licensing and not encumbered by any specific proprietary technology
- Inform and guide legislators and administrators

# Core Principles

- Verifiable paper ballots
- Matched e-Vote electronic records
- Electoral roll of voter participation
- Private and anonymous
- Secure 100% tallying and crosschecking
- Easy for citizens to understand

# Three Pillars of Trust

- Electoral Roll
  - managed by election officials and administered by voting staff
  - process designed to ensure anonymous vote
- Electronic voting records
  - generated by voter using voting system
  - digitally recorded and stored by voting system
- Matching Paper voting records
  - generated by voter using voting system
  - manually cast or mailed by voter

# Digital Trust and Logic Examined

- How can we ensure the machine does not cheat on the human operator who cannot “see inside”?
- MIT coined the term the “Frog Principle”<sup>\*</sup> for a multi-party *trusted logic process*
- If you have two parties that you cannot trust, how do you create a process that ‘hops’ between the two – in a way that if either cheats you will know?

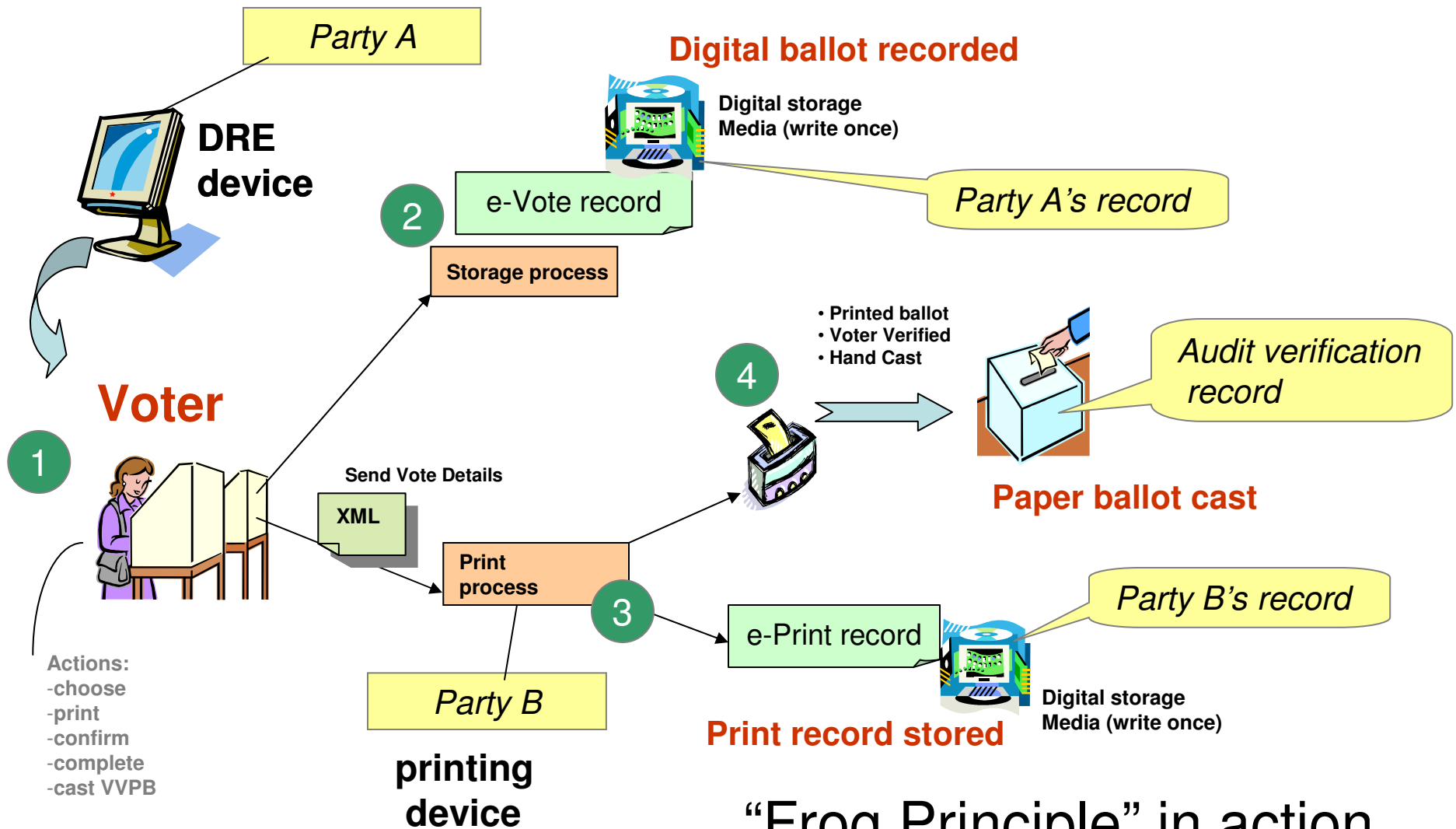
<sup>\*</sup>see: [http://www.vote.caltech.edu/media/documents/vtp\\_WP2.pdf](http://www.vote.caltech.edu/media/documents/vtp_WP2.pdf)

# Trusted Logic Process Explained

- **Uses write-once technology**
  - paper ballots (preferred medium today)
  - or “digital-paper” – liquid crystal plastic that machine “writes” to and human can read\*
  - or write-once digital chips that insert into a computer slot (MIT “frogs”)
- **First party creates record of the voters’ choices**
- **Voter transfers that information to second party**
- **Second party then confirms what the first party did and displays that information for the voter to confirm**
- **Process completes with three records retained**
  - What the first party said they did
  - The copy they passed to the second party
  - What the second party displays to the voter (printed as paper ballot)
- **Auditor can compare all three records – to ensure they match**

\* too costly today – but maybe within fifteen years time will be as cheap and easy to handle as paper.

# Creating a Trusted Exchange



“Frog Principle” in action

# Fundamentals of Trust

- 100% audit and comparison every time of all three Trusted Pillar counts to produce a certified election result
- Separation required between each step of the process; the trusted logic process is applied between the electronic and paper vote handling
- No single system can control or access more than one of the Trusted Pillars processing – each has to be distinct
- Every paper vote record is scanned and counted; every matching electronic vote is stored and then separately tallied

# Processing Layers

- Electoral roll and voter registration
- Voting process
- Counting process
- Verification and Certification
- Equipment deployment, setup and control

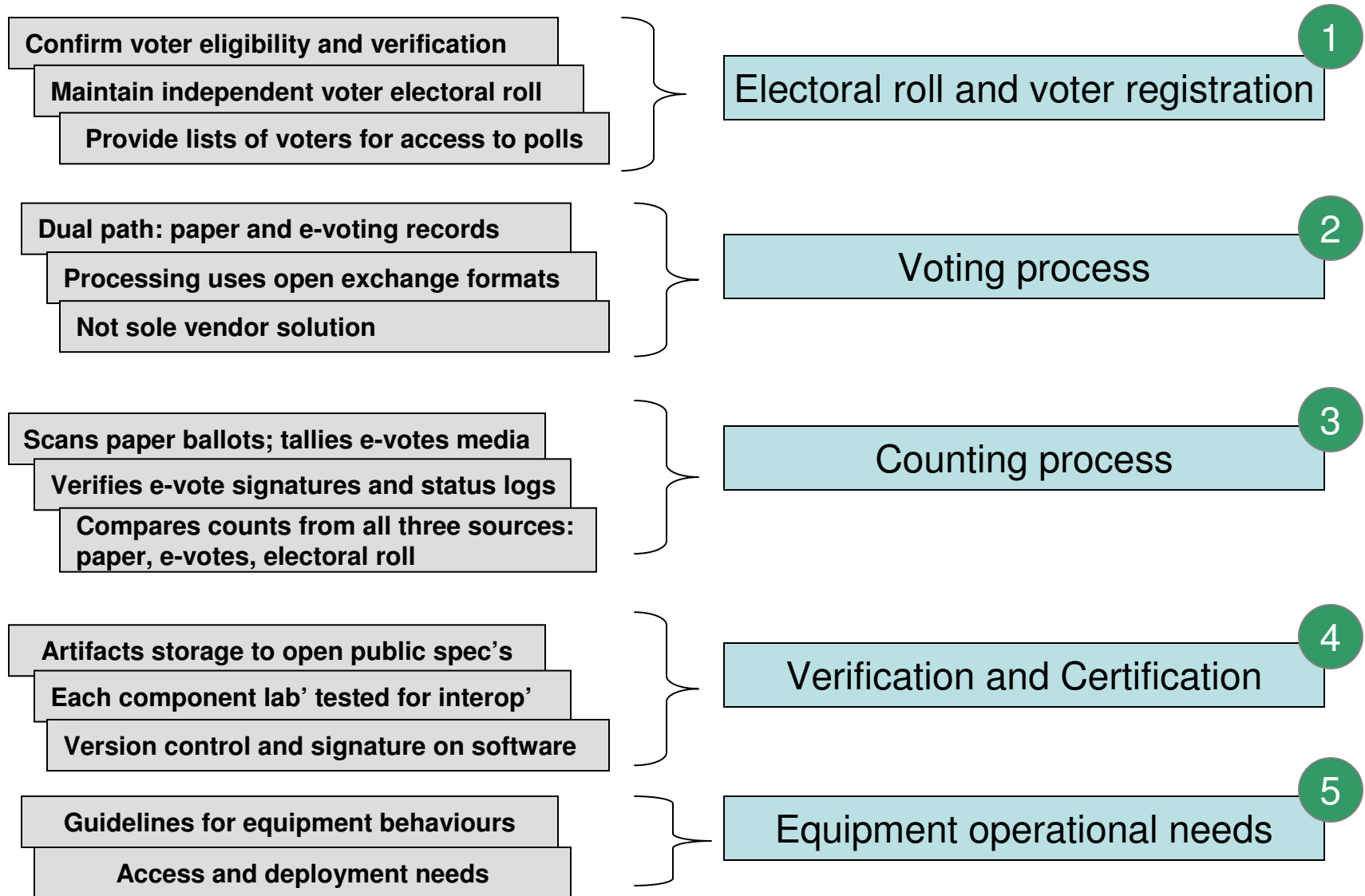
# Cornerstones of Process

- One provider cannot supply solutions across more than one layer or process
- Each layer must be autonomous and passes information to next layer in open formats that can be inspected and verified
- Software involved must be published to open source
- Physical separation of layers and devices associated with them

# Separation of Layers

- **Verifiable paper ballots**
  - Cast by hand or by mail by citizens directly
  - Printed / Formatted separately from e-Voting process (dual-path)
  - Electronic log of printing activity (implements “Frog principle”)
  - Allows machine scanning of paper ballots cast
- **Matched e-Vote electronic records**
  - Each vote record stored, not just rolling tally
  - Contains process status information (restartable)
  - Signature to enable authentication came from certified polling station
  - Anonymous - cannot identify voter
- **Electoral roll of voter participation**
  - Not accessible by e-Vote machines (stays private and anonymous)
  - Voter verification service and retains list of who votes and access codes
- **Secure tallying and crosschecking**
  - Independent service that compares totals and authenticates codes used
- **Easy for citizens to understand**
  - Localization and open access along with rules on formats of ballots

# Process Overview



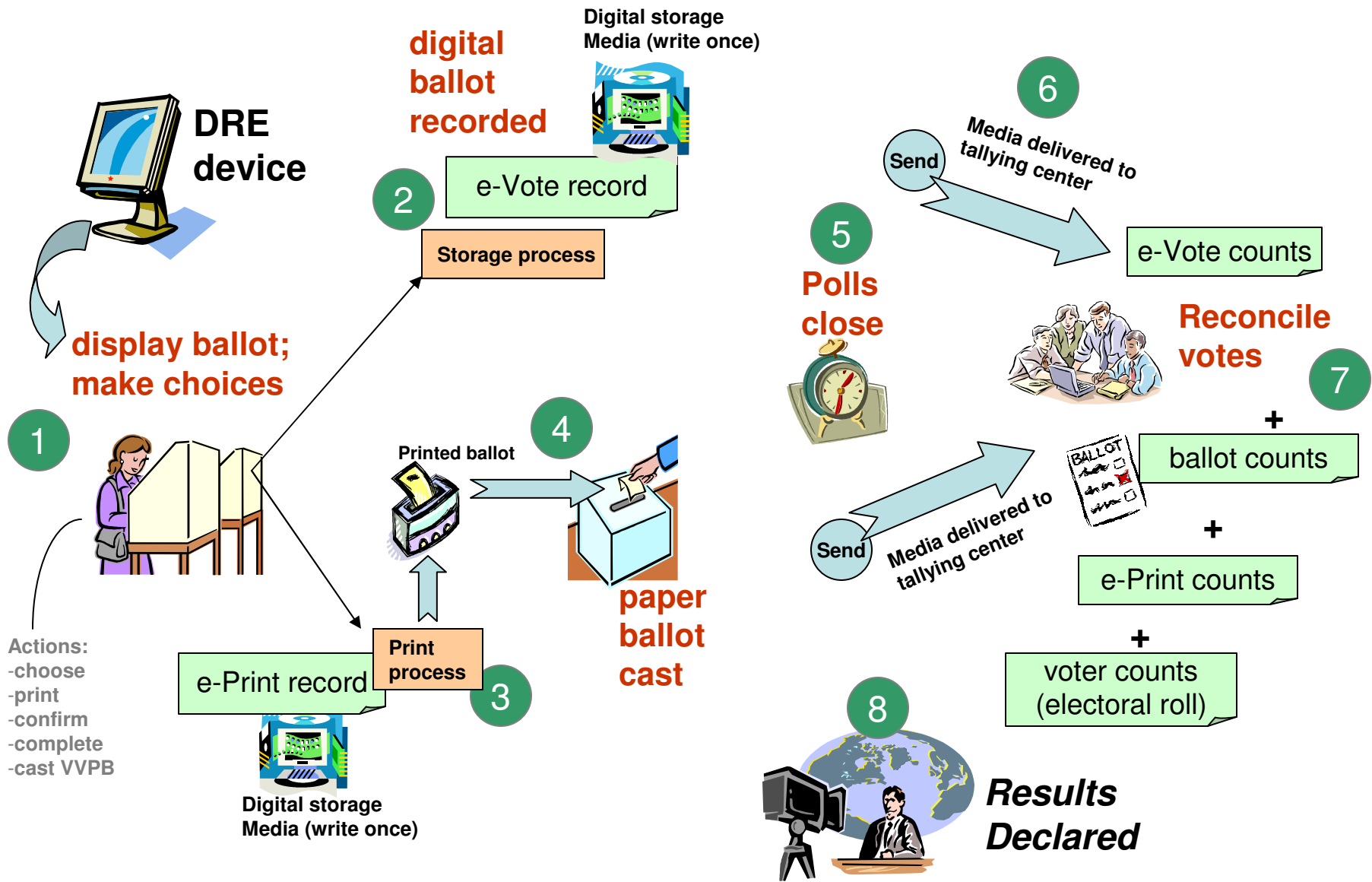
# Built-in Audit and Control

- Every single paper vote is scanned and counted and crosschecked against its matching eVote to give 100% verification and audit control (just like in a banking system)
- This can happen in a timely fashion after the ballot – and then fully verified results can be published that certify the election

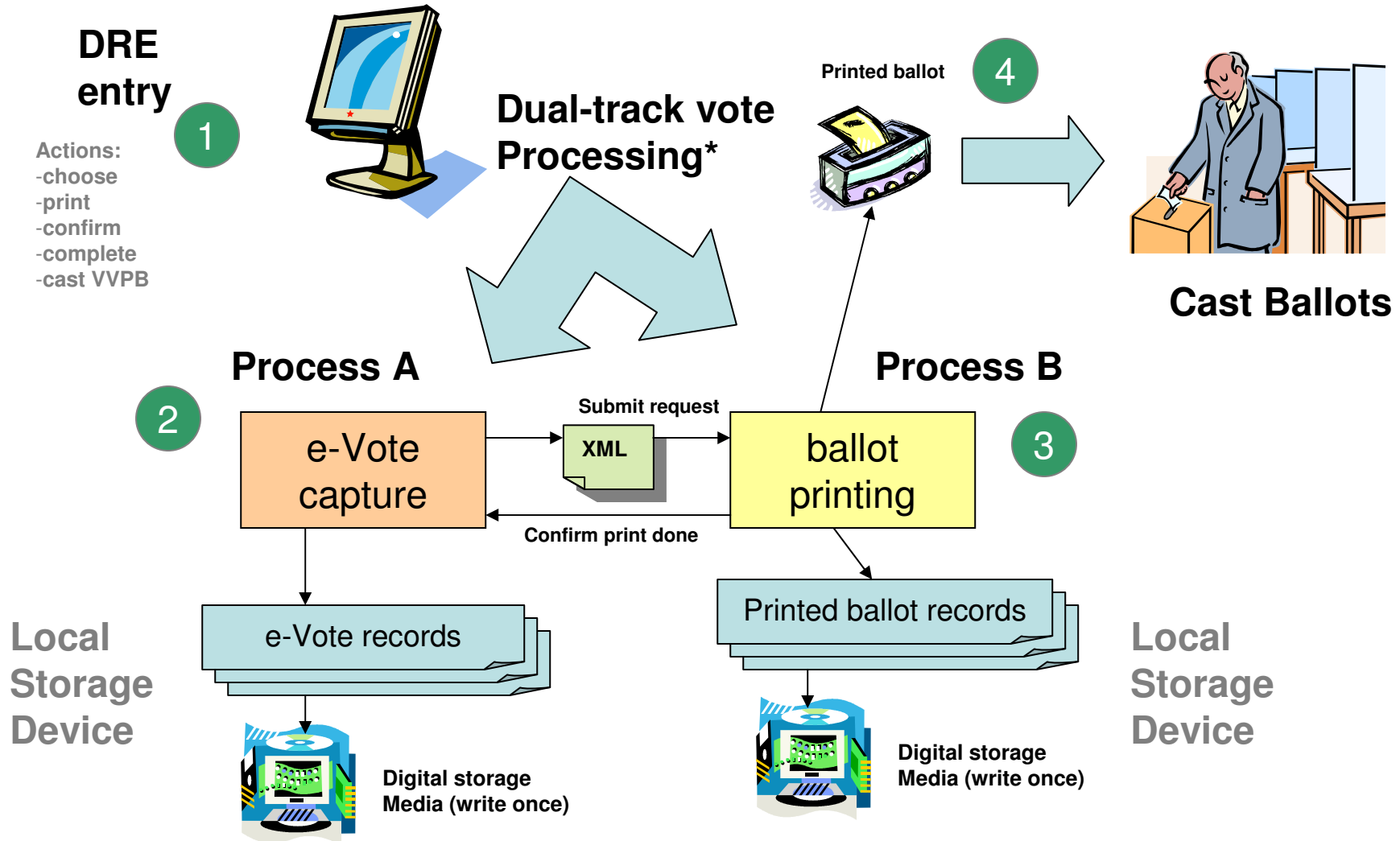
# Balancing information capture

- A trusted process allows the minimum effective information collection to effect a secure voting process
- Too much information compromises anonymous voting in subtle ways
- Too little information prevents effective audit trails
- The trusted process uses internationally agreed XML formats to manage information retention
- The process is rigorously designed to avoid retention of sequential event information that can compromise anonymous voting

# Process flow and separations

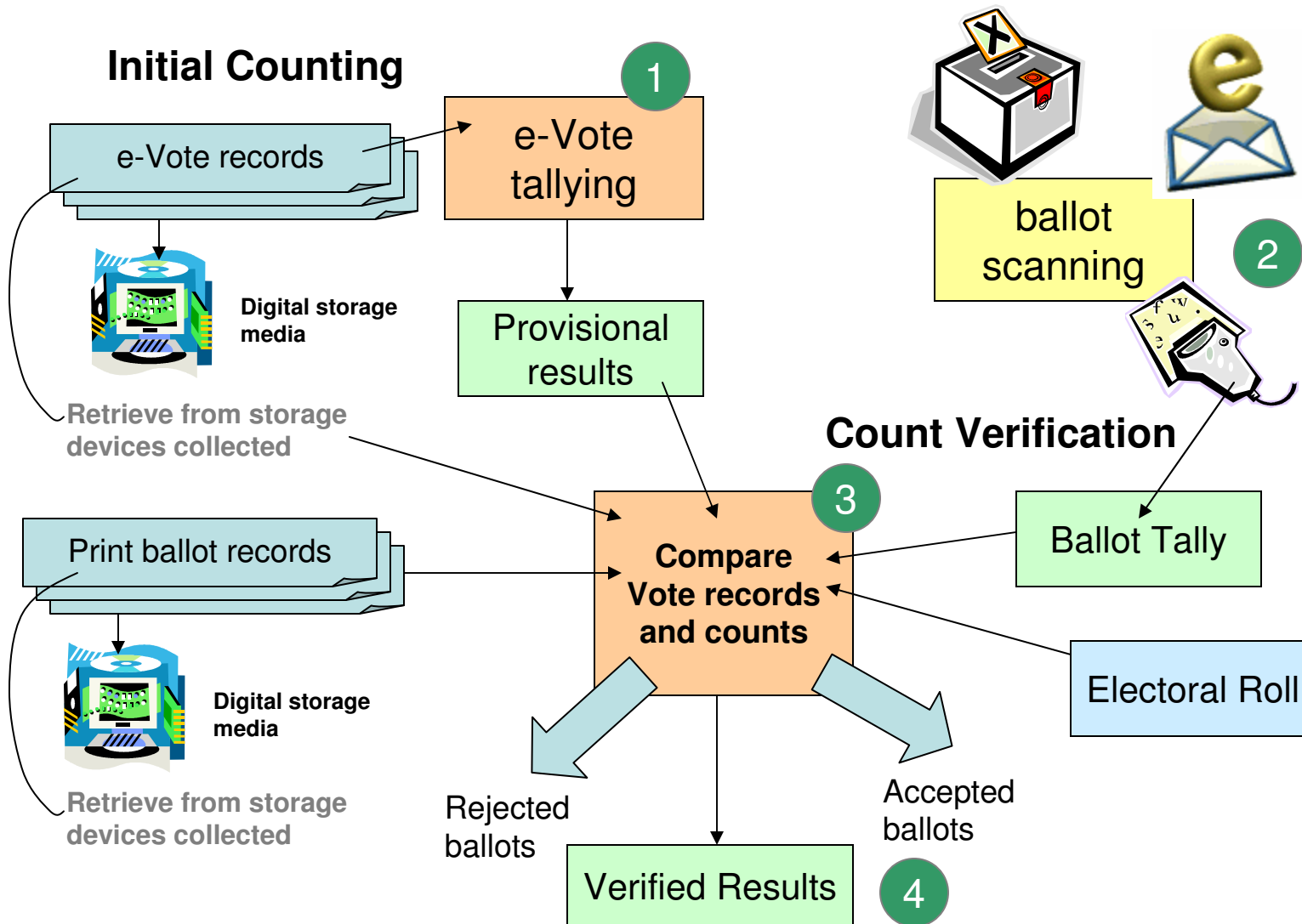


# Process Detail: Voting

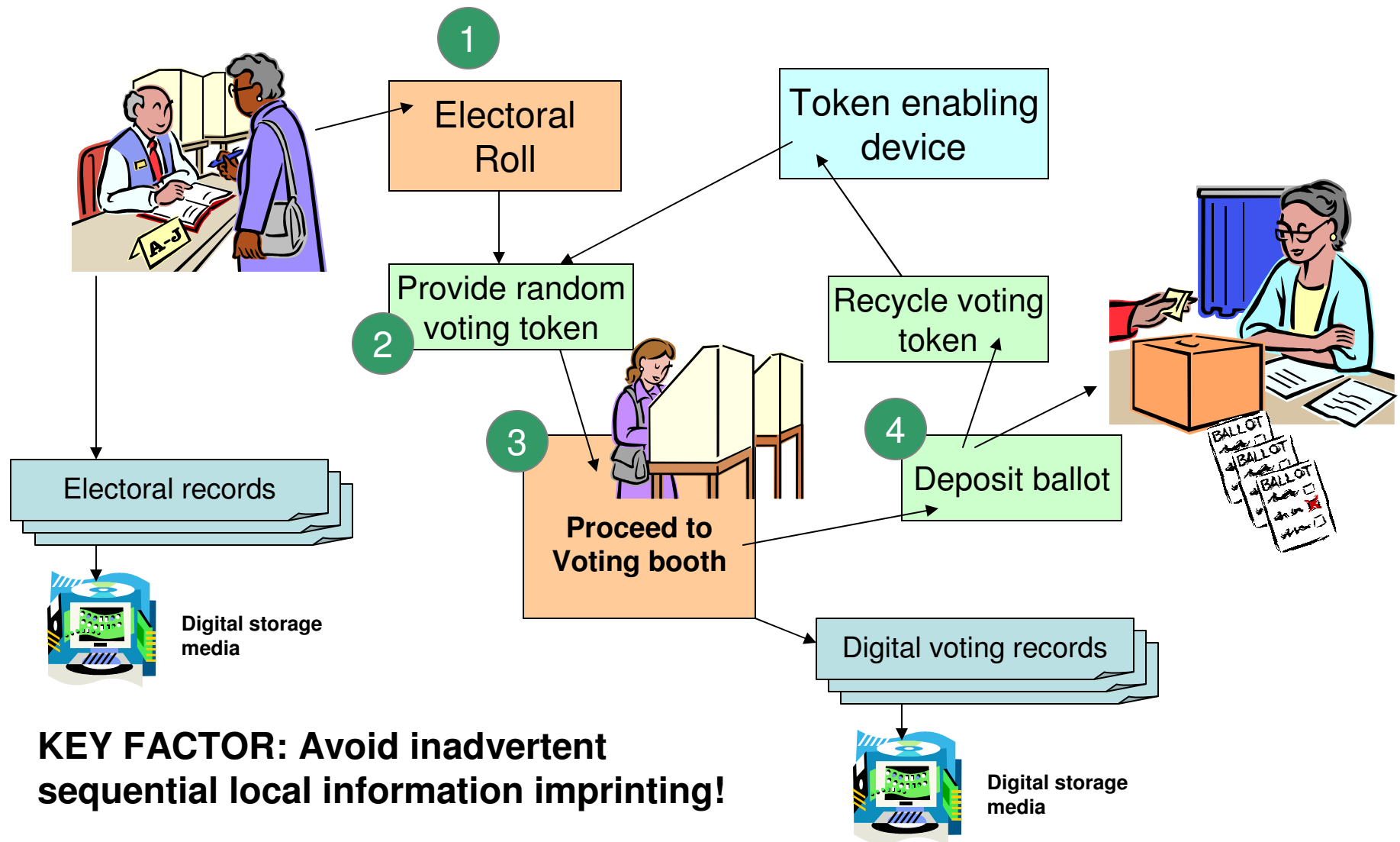


\* dual-track DV (direct verification) with storage implements the MIT "frog principle"

# Process Detail: Counting



# Process Detail: Voter Verification



**KEY FACTOR: Avoid inadvertent sequential local information imprinting!**

# Supporting Infrastructure

- Election officials have an obligation to provide trusted election services including:
  - accurate electoral rolls that are confidential (e.g. not sold like telephone white pages, mailing lists)
  - secure and safe voting environments - including polling stations, but beyond that to libraries and broader access for citizens generally
  - a trusted voting process to include independent verification of the ballot by trained government employed election staff using independently developed counting and verification tools.
  - ensure open source software that is inspected and only certified components are used in the voting process so that citizens can know that this is a trusted process
  - retain 100% copies of paper ballots, and write-once electronic media copies of e-Voting records, for minimum of one year following an election.

Sample overview of a voting process: <http://vote.nist.gov/TGDC/Process%20Model%2020050223.pdf>

# Summary

- Allows implementation of trusted process combining paper and digital ballots
- Overview of the core elements and their interactions, safeguards and cornerstones
- Mechanisms and separations to secure process and provide audit crosschecks
- XML required to run all the exchanges
- Goal – produce open public specification

# Useful Resources

- Website of Professor Rebecca Mercuri - <http://www.notablessoftware.com/evote.html>
- Brookings Institute Report - Agenda for Election Reform - <http://www.brook.edu/comm/policybriefs/pb82.htm>
- CalTech site on ensuring voting integrity - <http://vote.caltech.edu/reports>
- NYVV - Advantages of ballot scanners over DREs - <http://www.nyvv.org/paperballotVsDRE.htm>
- Analysis of counting irregularities in US elections - <http://ideamouth.com/voterfraud.htm>
- MIT Study on accuracy of voting systems - [http://vevo.verifiedvoting.org/vendors/studies/20040601\\_Ansolabeherpaper.pdf](http://vevo.verifiedvoting.org/vendors/studies/20040601_Ansolabeherpaper.pdf)
- Verified Voting site <http://www.verifiedvoting.org>
- West Virginia procedures for optical scanning ballots - <http://www.wvsos.com/elections/eday/procedureselectronic.htm>
- Administration and Cost of Elections (ACE) - <http://www.aceproject.org/main/english/index.htm>
- Anecdotal reporting on 2004 US elections - <http://www.lionsgrip.com/voting2004.html>
- NIST Glossary of Terms document – [http://vote.nist.gov/TGDC/voting\\_glossaryv2Feb28.doc](http://vote.nist.gov/TGDC/voting_glossaryv2Feb28.doc)