



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

July 1, 2005



Trusted Logic Voting Systems with OASIS EML 4.0 (Election Markup Language)

Presenter:
David RR Webber
Chair OASIS CAM TC
<http://trustedelections.org>



Contents

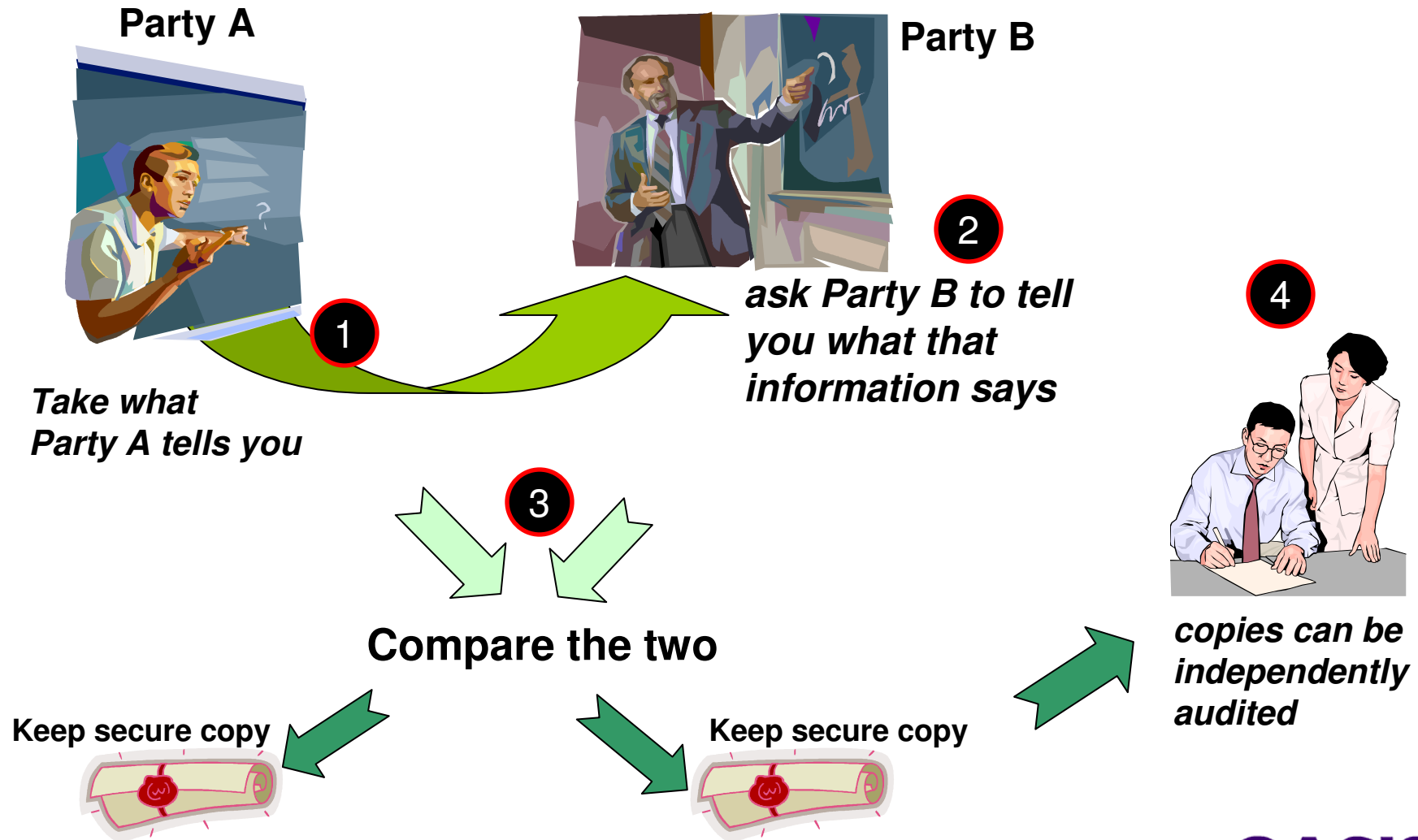
- **Trusted Logic Voting (TLV)**
 - Needs, Approach and Implementation
- **Using OASIS EML**
 - History, Overview, Processes, Transactions
- **Applying OASIS EML**
 - Example process steps and actions
 - Supporting US-style elections
- **Summary**

Trusted Logic Voting Needs

- How can we ensure the voting machine does not cheat on the human operator who cannot “see inside”?
- How can we know that every vote is counted as cast?
- If you have two parties that you cannot trust, how do you create a process that works between the two – in a way that if either cheats you will know?
- How can you create an audit trail that allows 100% crosschecking while keeping voter privacy?
- Use existing work in the field on multi-party *trusted logic process* (e.g. MIT approach using the “Frog Principle”*)

*see: http://www.vote.caltech.edu/media/documents/vtp_WP2.pdf

Trusted Logic Concept

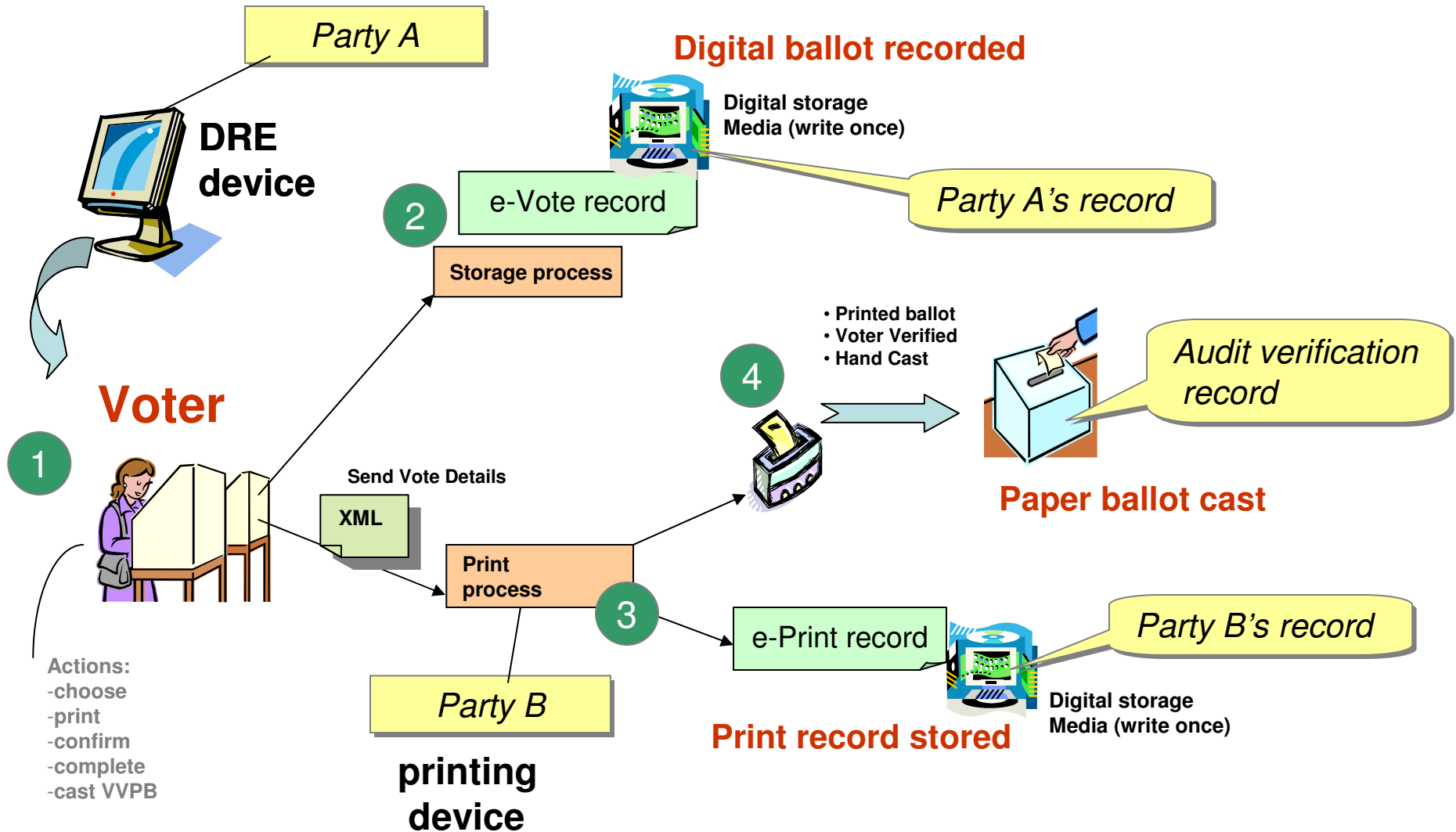


Trusted Logic Applied to Voting

- **First party creates record of the voters' choices**
- **Voter selection information transferred to second party**
- **Second party then confirms what the first party did and displays that information for the voter to confirm**
- **Confirmation 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”)
- **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.

US Voting System Example



- *Trusted Logic Voting in action* -

Core Trust 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
- Uses secure open source computer system

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

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

Making Secure Computing

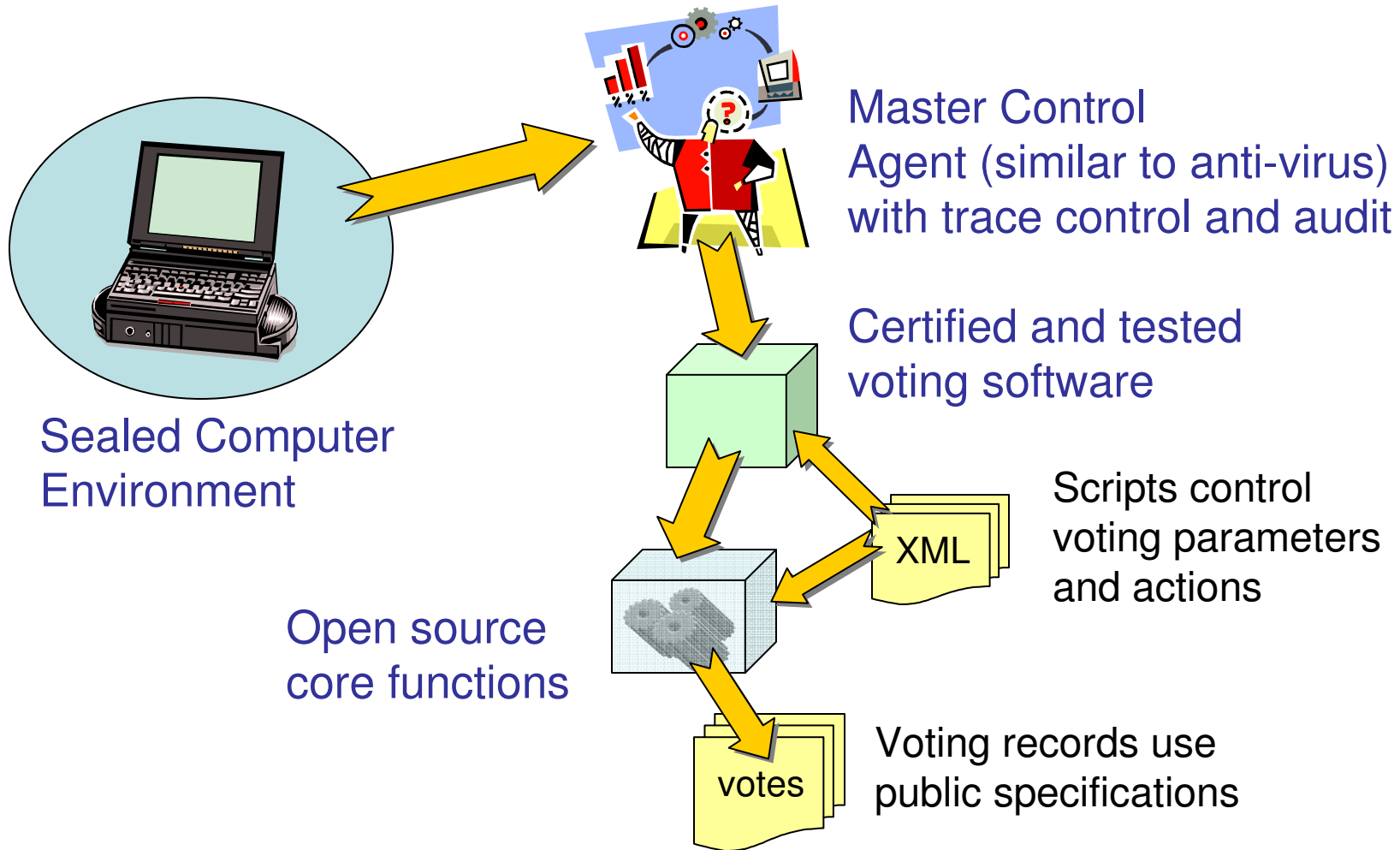
- Process uses open public specifications
- Logic and control parameters implemented as scripts that are hand-edited and verified
- Core vote handling software components are open source
- Implements secure operating environment (similar to anti-virus control) with locked master control execution agent to ensure correct components are running unmodified at all times
- Certified closed and locked hardware environment to safeguard against unauthorized intrusions

Designed to Mitigate Attacks

- **Attack Characteristics:**
 - a launch platform;
 - a manipulation method;
 - an activation method;
 - a cheating heuristic.
- **Attack methods**
 - vote presentation
 - vote record shifting
 - ballot stuffing
 - count manipulation
 - denial of service
- **Attack delivery**
 - direct access allows install to occur
 - mal-ware loader replaces part or all of software (like virus)
 - hardware loader from card or component
 - trigger mechanism
 - network or remote device access



Example Secure Computing



(see slide 18 for more details)

Ensuring Timely Results

- To be trusted elections must be able to produce timely and accurate answers and results
- 100% audit and comparison of three counting sources provides this direct analysis of voting counts immediately after the balloting closes
- Avoids recrimination, legal challenges and uncertainty that is introduced by today's partial audits only
- Identifies and traces operational issues (machine problems or operator errors) and resolves them
- Allows confidence in declared results of elections

Balancing information capture

- A trusted logic 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
- Example: stamping votes with machine IDs – good idea or bad idea?
- Next we look at how OASIS EML 4.0 instructs on the information exchange details...

Ensuring Vote Process Consistency

- Use of XML voting structures for election artifacts and XML scripts to monitor and control voting process
- Use established international specifications for XML voting records – OASIS Election Markup Language (EML)
- Allows consistent verification and certification testing of any voting system
- Enables development of open source components of known behaviour to underpin election solutions
- Makes interoperability between vendors equipment possible (scanners, printers, counting)

Quick Overview of EML



- History

- Work begun in May 2001 in the USA and UK
- Charter: To develop a standard for the structured interchange of data among hardware, software, and service providers who engage in any aspect of providing election or voter services to public or private organizations
- UK government has implementations:
 - UK Local Election pilots held in May 2003.
- <http://www.oasis-open.org/committees/election>

- Council of Europe Endorsement



- Council of Europe Ministers have endorsed the e-voting recommendations and with that the use of EML
<http://europa.eu.int/ida/en/document/3294/358>

- EML 4.0 is a committee draft for review and comment, other countries in Europe now exploring use, Spain, Swiss ...

Overview of EML and processing: <http://www.idealliance.org/papers/xml03/slides/spencer/spencer.ppt>



Category Overview of EML

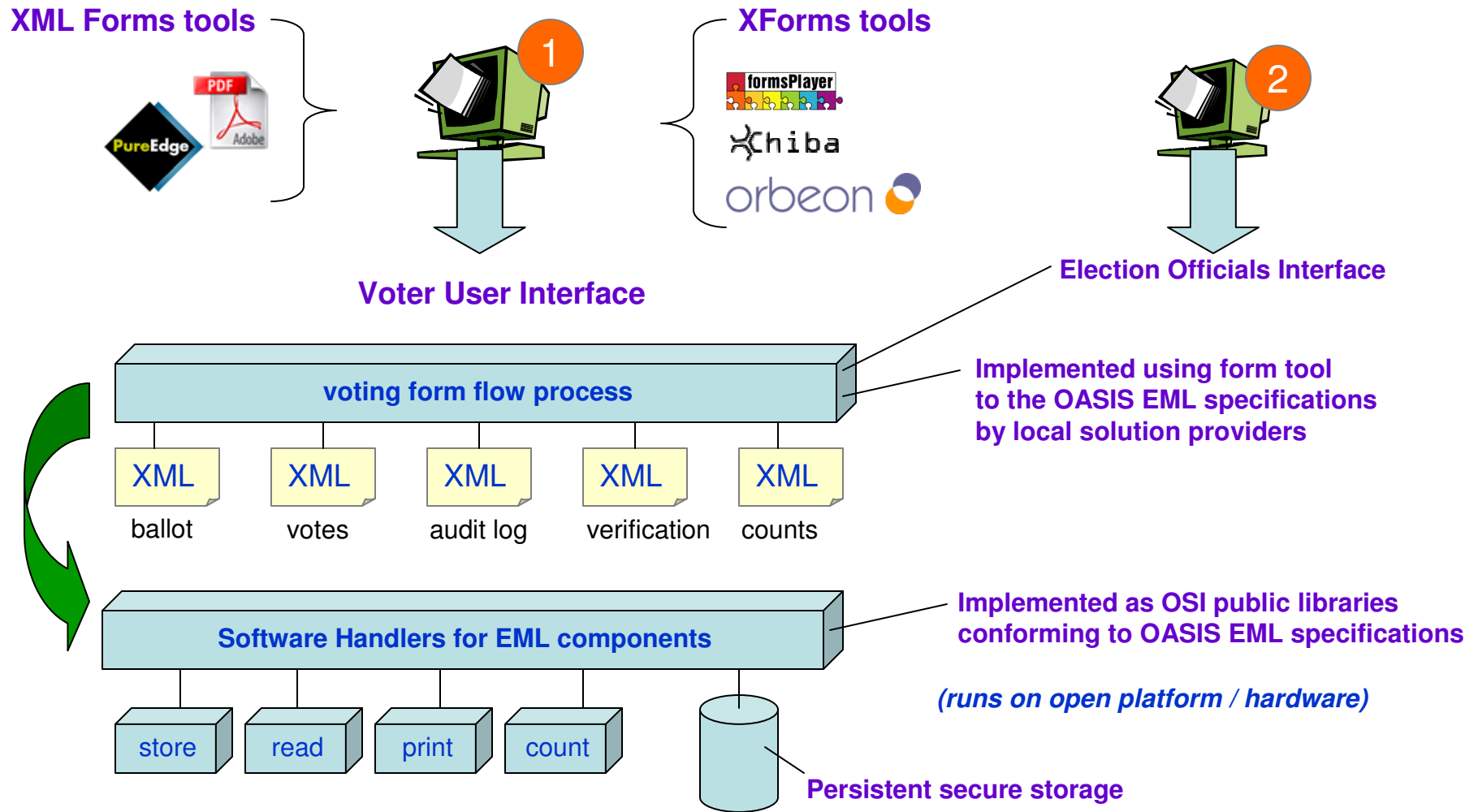
One or more XML schemas series are provided to support each general process area:

- Pre election
 - Election (100)
 - Candidates (200)
 - Options (600)
 - Voters (300)
- Election
 - Voting (400)
- Post election
 - Results (500)
 - Audit
 - Analysis

Some functions belong to the whole process and not to a specific part:

- Administration Interface
- Help Desk

Solution Components for EML



OASIS initiative forming to develop OSI components for EML processes

OSI Base Handler Components

1. LOADER –

- transfers EML 440 records from digital media and inserts them into database, or secure storage area, creates or reads EML 460. Creates EML 480 access audit entry.

2. READER -

- loops thru EML 440 records in storage area.
 - a) opens record and verifies digital signature
 - b) extracts voting information from 440
 - c) updates ballot totals
 - d) writes access audit entry EML 480

3. PUBLISH –

- creates EML 510 election result record in XML.

4. DISPLAY-

- outputs EML 520 details to printer / screen, etc in language of choice.

5. TESTER –

- checks EML formats for valid content. Check digital signature / certificate handling

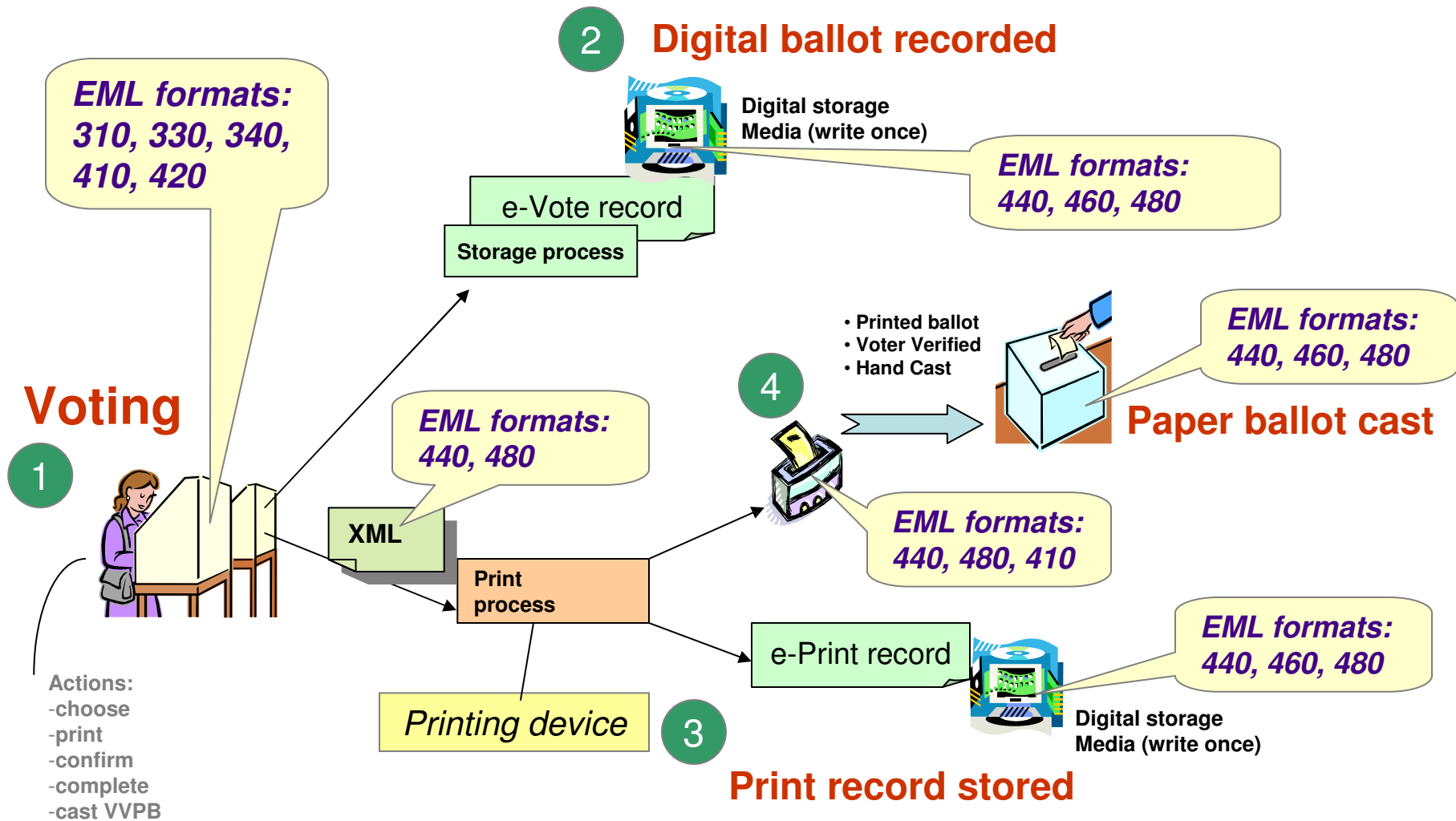
Selected EML 4.0 Transactions

Schema Name	Purpose
EML 110 – election event	Information about an election or set of elections. It is usually used to communicate information from the election organizers
EML 210 – candidate nomination	Used to nominate candidates or parties, consenting or withdrawing
EML 230 – candidate list	Contest and candidates details
EML 310 – voter registration	Used to register voters for an election
EML 330 – voter election list	Details of actual voters for an election
EML 340 – polling information	Notification to voter of an election, their eligibility and how to vote
EML 410 – ballot	Describes the actual ballot to be used for an election
EML 420 – voter authentication	Used for voter authentication during a voting process
EML 440 – cast vote	Actual record of vote cast
EML 460 – votes group	Group of votes being transferred for counting
EML 480 – audit log	Documents access to voting records and reason
EML 510 - count	Results of election contest(s) and counts
EML 520 - result	Communicating specific result details on candidates and elections

OASIS EML 4.0 transaction use

- Electoral Roll (**EML 310, 330, 340**)
 - managed by election officials and administered by voting staff
 - process designed to ensure anonymous vote
- Electronic voting records (**EML 440, 460, 480, 510**)
 - generated by voter using voting system
 - digitally recorded and stored by voting system (**EML 510**)
- Matching Paper voting records (**EML 440, 480**)
 - generated by voter using voting system
 - manually cast or mailed by voter
 - scanned electronically (**EML 440, 480, 510**)

EML and US Voting Example



- Using EML formats in action -

Reality of real-world voting

- Good solutions have to be adaptive and survive in a complex unpredictable world; they have to administer well
- Today's paper-based voting methods have a culture around them and years of operational lessons learned
- Need to have formalized documented procedures
 - Council of Europe Ministers have endorsed the comprehensive steps for e-voting recommendations and with that the use of EML <http://europa.eu.int/ida/en/document/3294/358>
- Expecting 100% perfection is unrealistic; trusted system has to be a best case – that allows people to be able to diagnose events and occurrences, e.g.:
 - someone forgot a voting card left in a voting machine
 - the machine jammed; the disk is unreadable
 - someone keyed in the wrong setup code
 - the computer hardware failed

EU Procedures* (Processing Layers)

Items covered:

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

*see: http://www.coe.int/T/e/integrated_projects/democracy/02_Activities/02_e-voting/01_Recommendation/default.asp#TopOfPage

EU Procedures – clarifying items (1)

These trusted logic items should be added:

1. Explicit reference to the importance of using write-once media for vote recording - either paper or digital
2. Need for voters to be able to physically verify their vote directly - via paper ballot or equivalent physical representation of an actual ballot - not an electronic ephemeral representation, and to cast that physical representation by hand
3. Need to separate the layers of the process - so the same component provider is not doing all vote creating, printing, and counting the total votes (no single solution provider)
4. Need to use trusted logic principle so that the voter can verify that the digital voting choice recorded matches the physical voting choice they selected

EU Procedures – clarifying items (2)

These ballot processing items should be added:

5. Need to compare 100% of all counts - electronic and physical ballot counts and electoral record counts to ensure they tally*
6. Explicit call-out of the need to avoid sequential processing information compromising vote privacy and anonymity
7. Explicitly call-out that overall election counts should be tallied independently for each of the sources - electoral roll, digital votes, and voter verified (paper) ballot counts (after scanning - EBI - Electronic Ballot Imaging**).

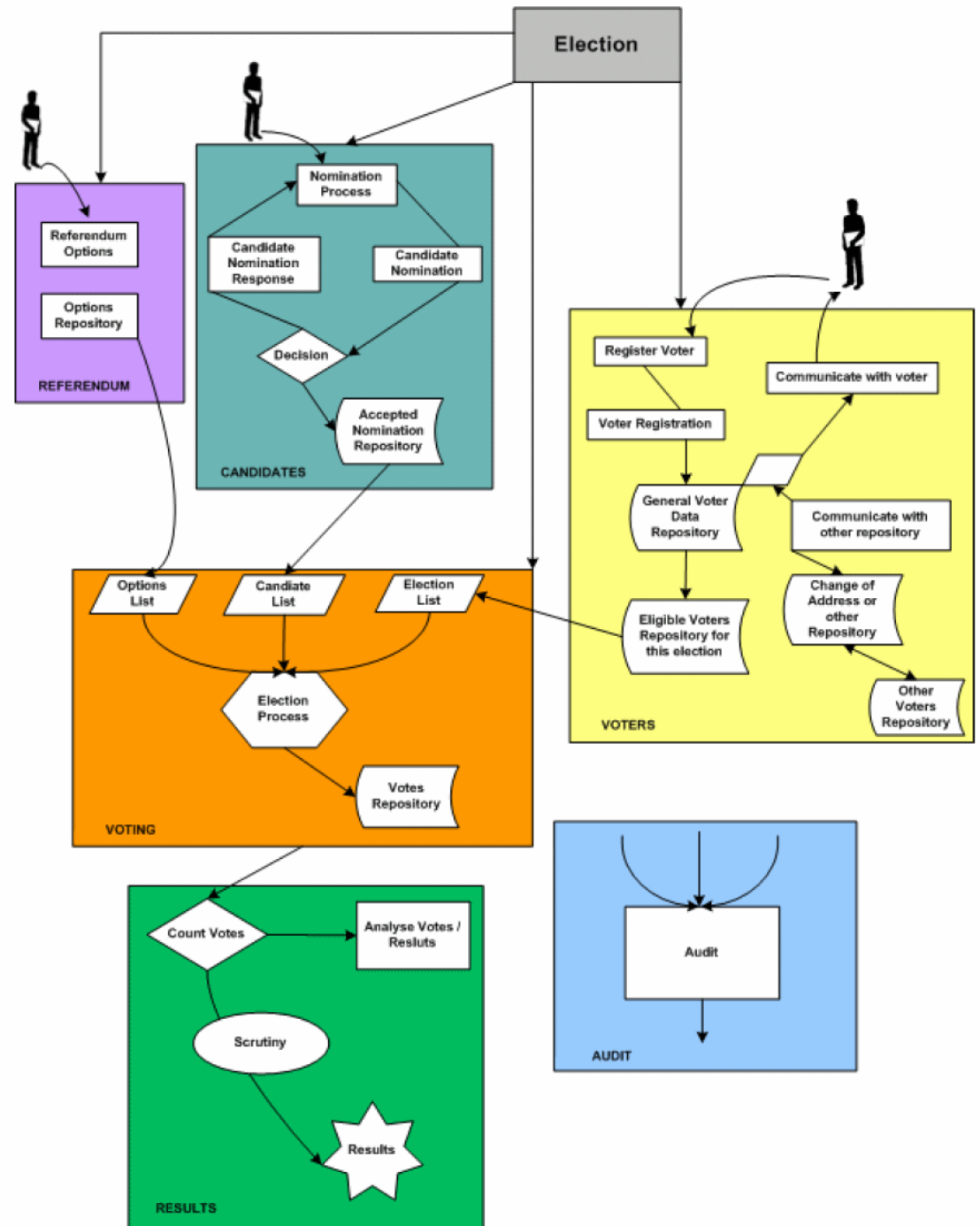
* More in-depth technical operation level discussions here:
<http://gnosis.cx/publish/voting/privacy-electronic-voting.pdf>

** Electronic Ballot Imaging - <http://www-128.ibm.com/developerworks/xml/library/x-matters36.html>

How OASIS EML views process steps and separations

Election:

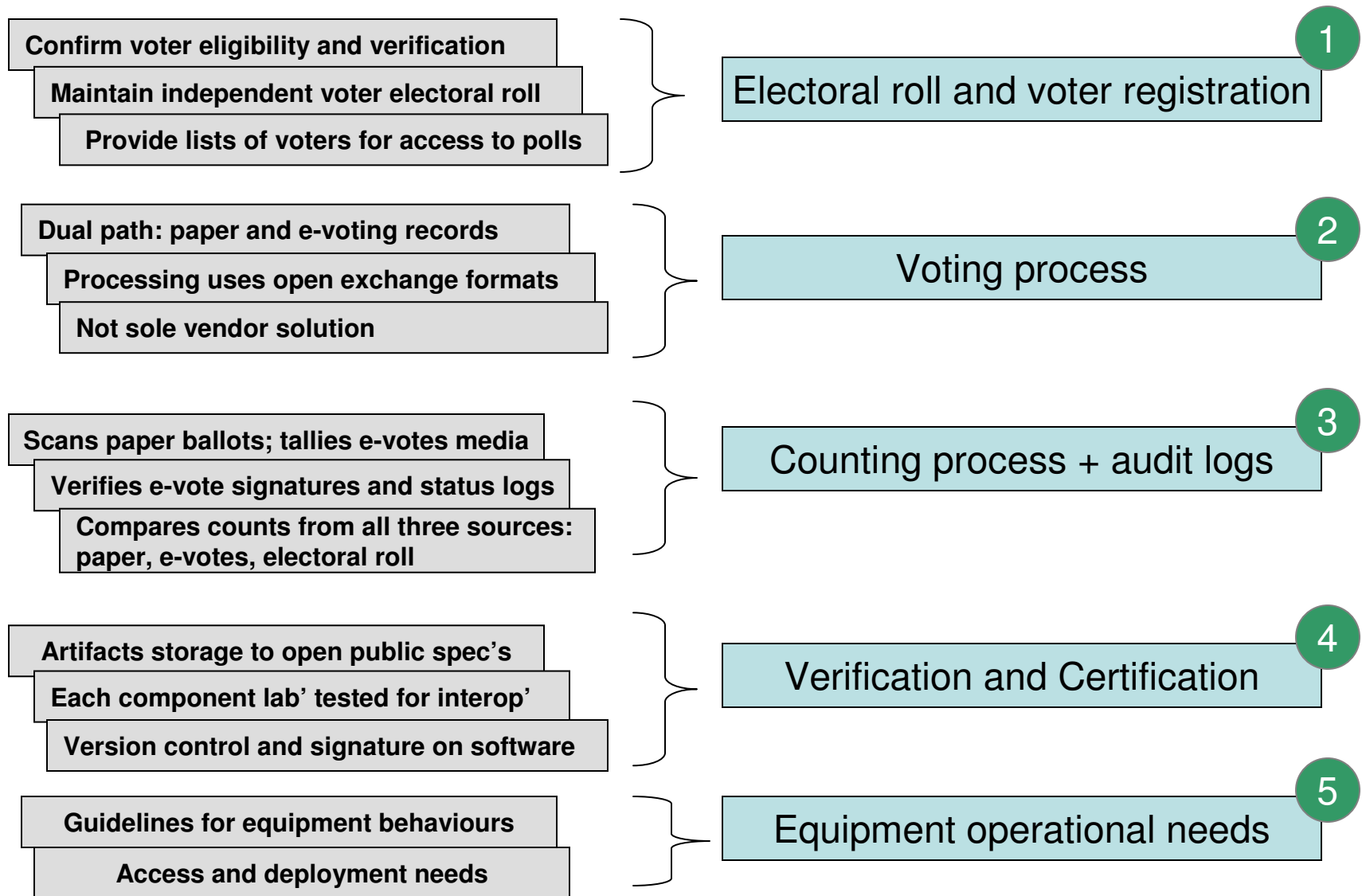
- Candidates
- Ballot / Referendum
- Voters
- Voting
- Results
- Audit



Procedural requirements

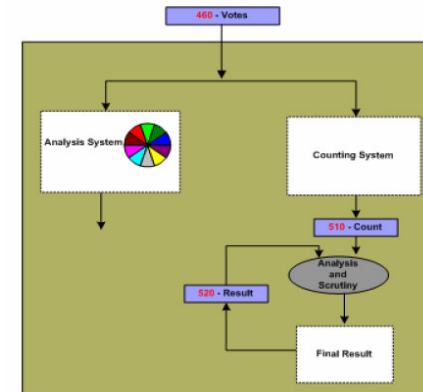
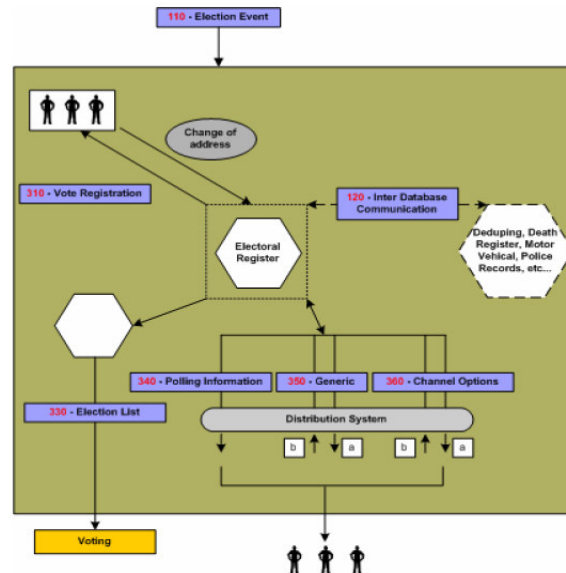
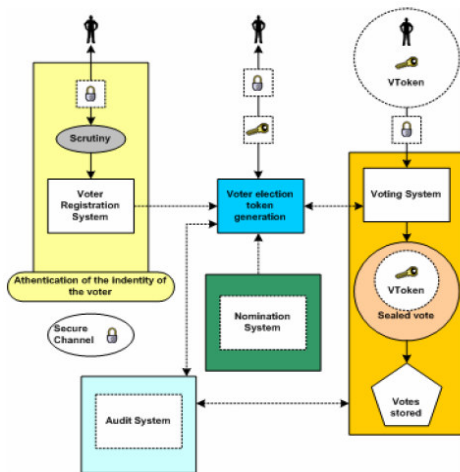
- One implementer cannot supply solutions across more than one layer or process
- Each layer must be autonomous and passes information to next layer in open formats that can be inspected and verified
- Software involved must be published to open source
- Physical separation of layers and devices associated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

Process Overview



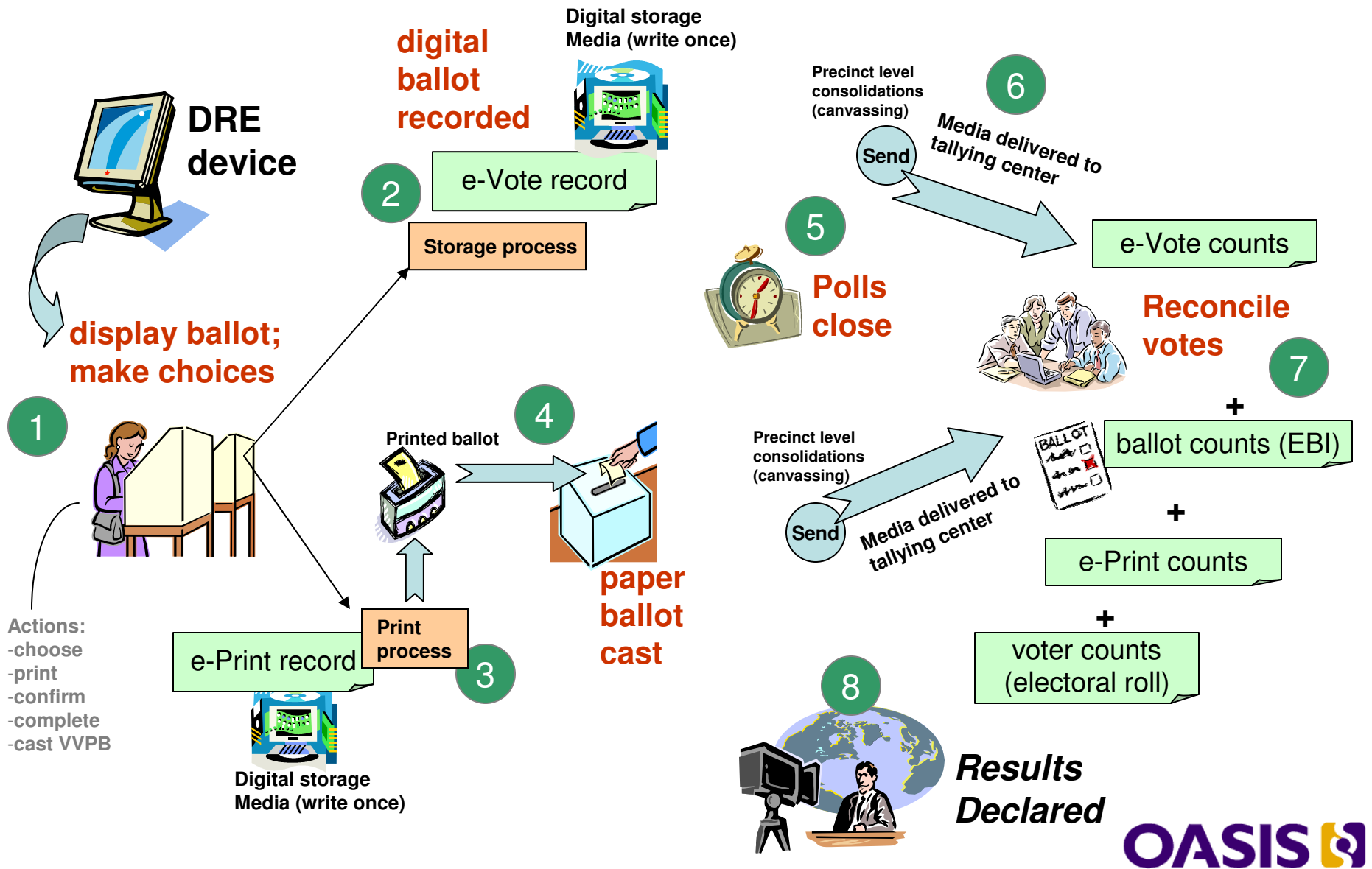
OASIS EML process details

- The OASIS EML provides details for each part of voting process (see specification for exact details)
- Next few slides show how these can be applied to a trusted logic voting process

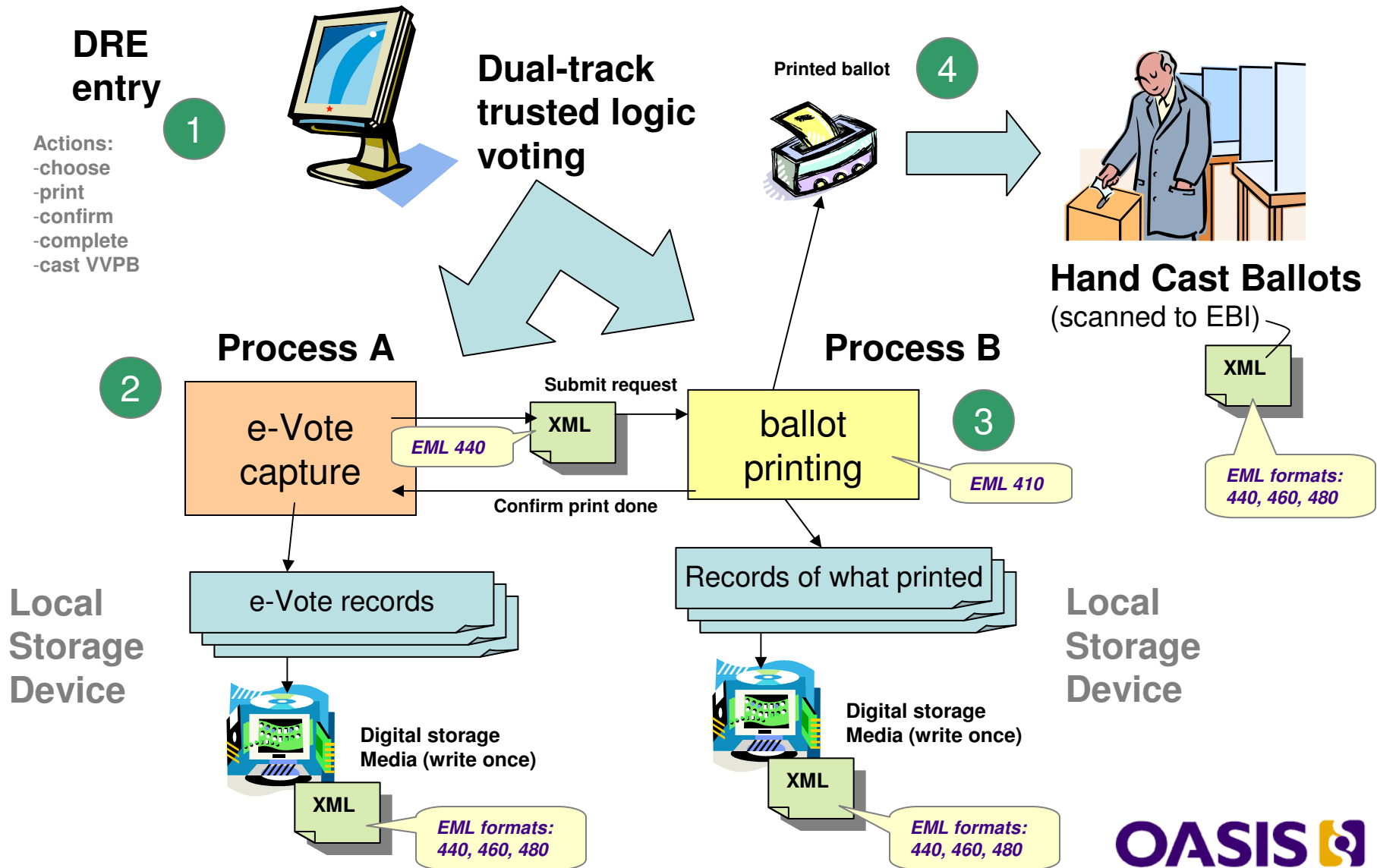


more process details – NIST / HAVA: <http://vote.nist.gov/TGDC/Process%20Model%2020050223.pdf>

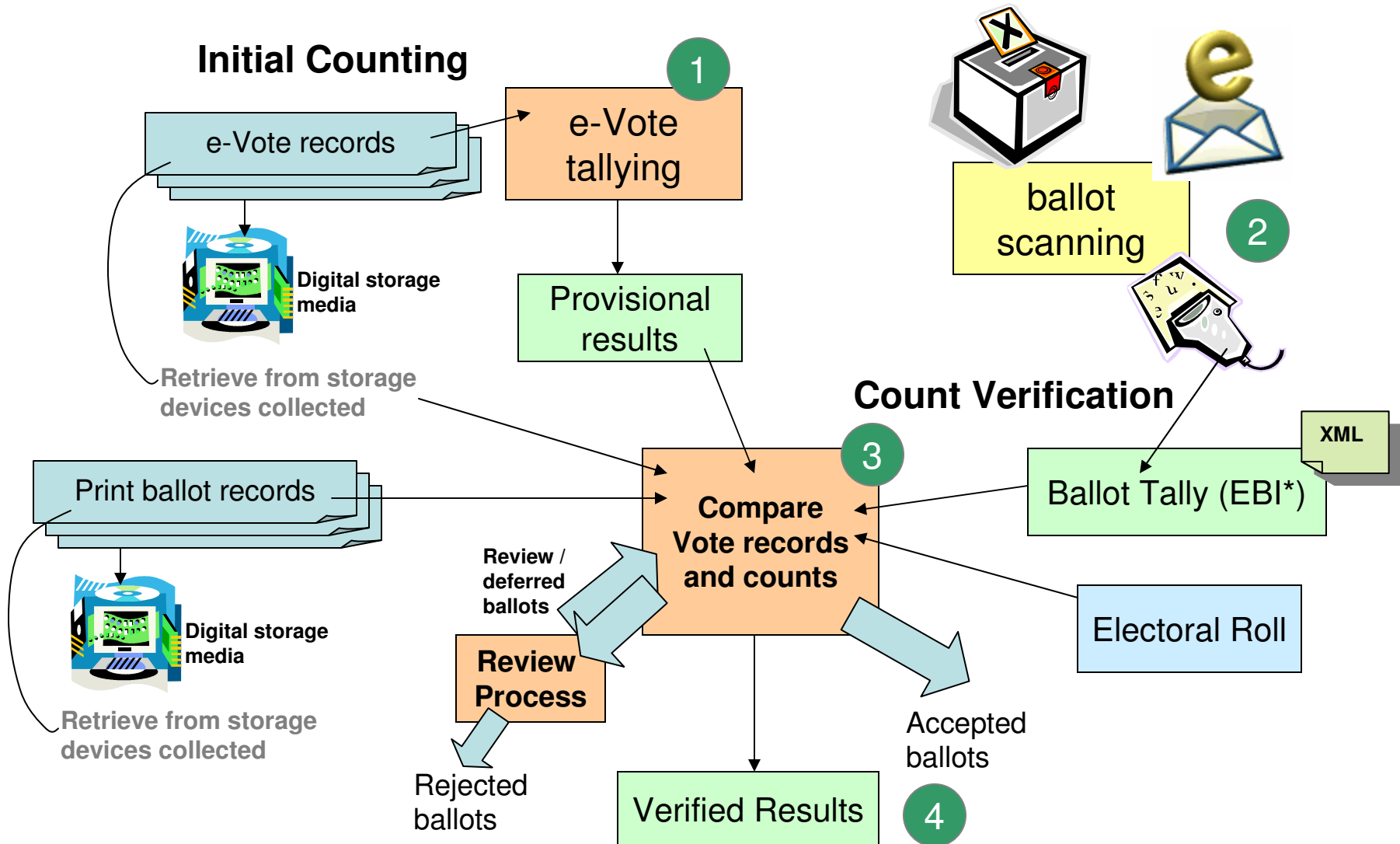
Projected US implementation flow



Action Process : Voting

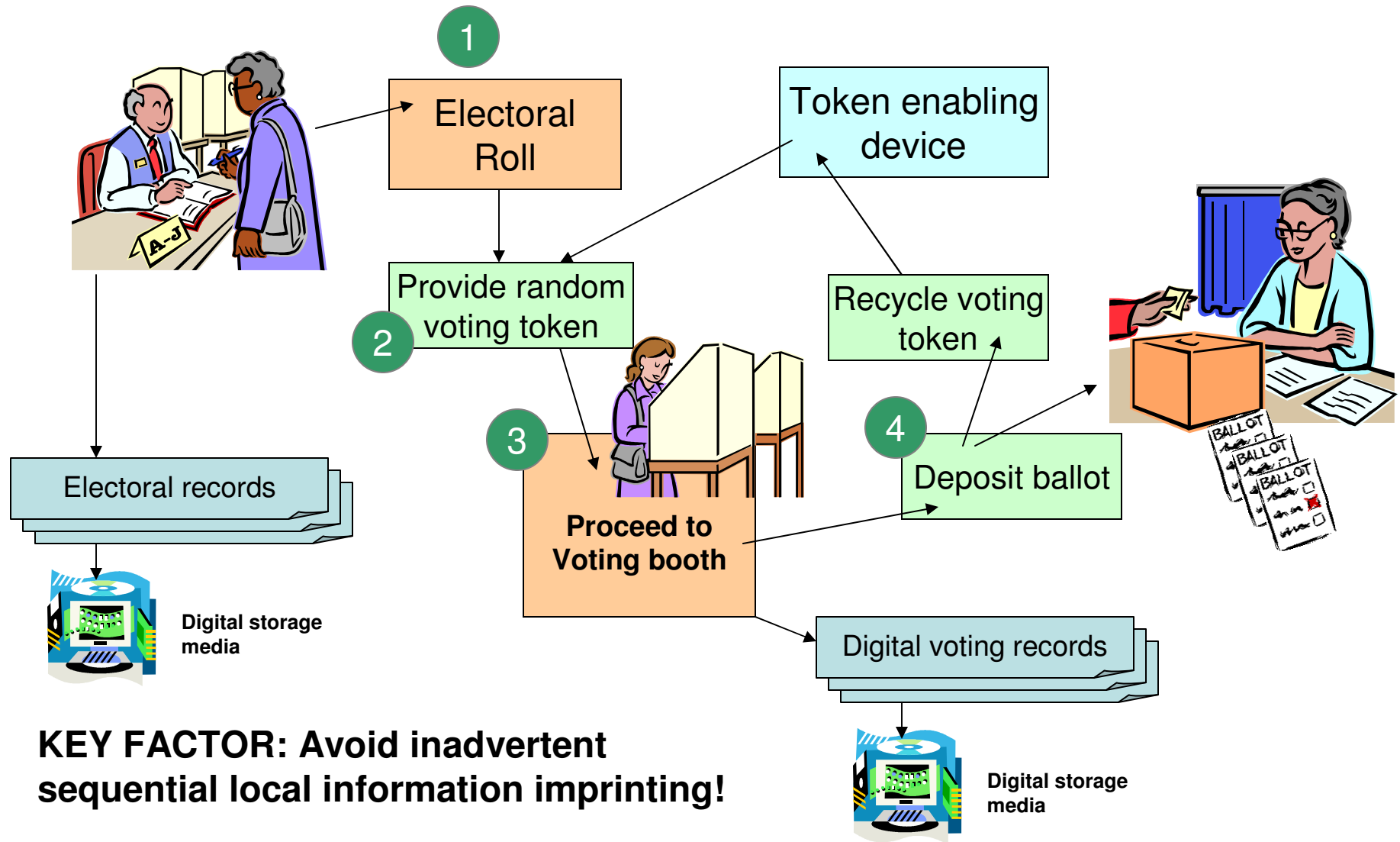


Action Process : Counting



*Electronic Ballot Imaging - <http://www-128.ibm.com/developerworks/xml/library/x-matters36.html>

Action Process : Voter Verification



Creating an open marketplace

- Open *trusted logic voting (TLV)* 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

TLV Implementation Components

1. Voter registration and ballot day sign-in - separate system, with separate counts and reporting at end of day. Provides voters with access to voting system to cast their ballot; uses OASIS EML formats
2. Separate Voting system that voters access to select choices, make vote, passes choices to VVPAT printing system, creates electronic record of vote (uses simple ballot-ID to provide crosscheck and real-time auditing). Supports disabled access and multilingual access.
3. Ballot printing system - creates paper record, and printing audit electronic record. Voter confirms paper ballot detail, and casts vote into ballot box. Ballot-ID printed on ballot; ballot is scanned into EBI*.
4. Immediate counting - after polls close – provides 100% crosscheck via ballot-ID between counts from 1), 2) and 3). Takes OASIS EML records and counts them. Counting software is open source. Using 3 separate count systems – gives banking system level of robust auditing and trust.
5. The goal is to provide the underlying functions as OSI - and then allow solution providers to provide localization and value-add above that using the form tools of their choice.

* EBI – electronic ballot image (EML 440)



Comparison Matrix

Feature	TLV	Optical Scan	DRE	VVPAT	VVAATT
Voter verified cast paper ballot	Yes	Yes	No	Partial	No
Two step separate vote verification count	Yes	Yes	No	No	Partial
Three step voting count 100% crosscheck	Yes	Partial	No	No	No
Provides rapid vote remediation / auditing	Yes	Yes	No	No	No
Highly resistant to ballot stuffing attacks	Yes	Partial	No	Partial	Partial
Highly resistant to ballot switching attacks	Yes	Partial	No	No	Partial
Blind voter environment support	Yes	Partial	Yes	Partial	Yes
Deaf voter environment support	Yes	Yes	Yes	Yes	No
Multilingual voting support	Yes	Partial	Yes	Yes	Partial
Supports internationally developed process	Yes	Partial	No	No	No
XML used to record and script voting	Yes	Partial	No	No	No
Conformance suite for implementations	Yes	No	No	No	No
Digital certificates and encryption	Yes	No	Yes	Yes	Yes
Uses VoiceXML for audio verification	Yes	Partial	No	No	Partial
Open source API and SDK	Yes	No	No	No	No
Uses off-the-shelf computer equipment	Yes	Yes	No	No	No
Provides secure computing environment	Yes	No	No	No	No
	17:17	9:17	4:17	5:17	5:17

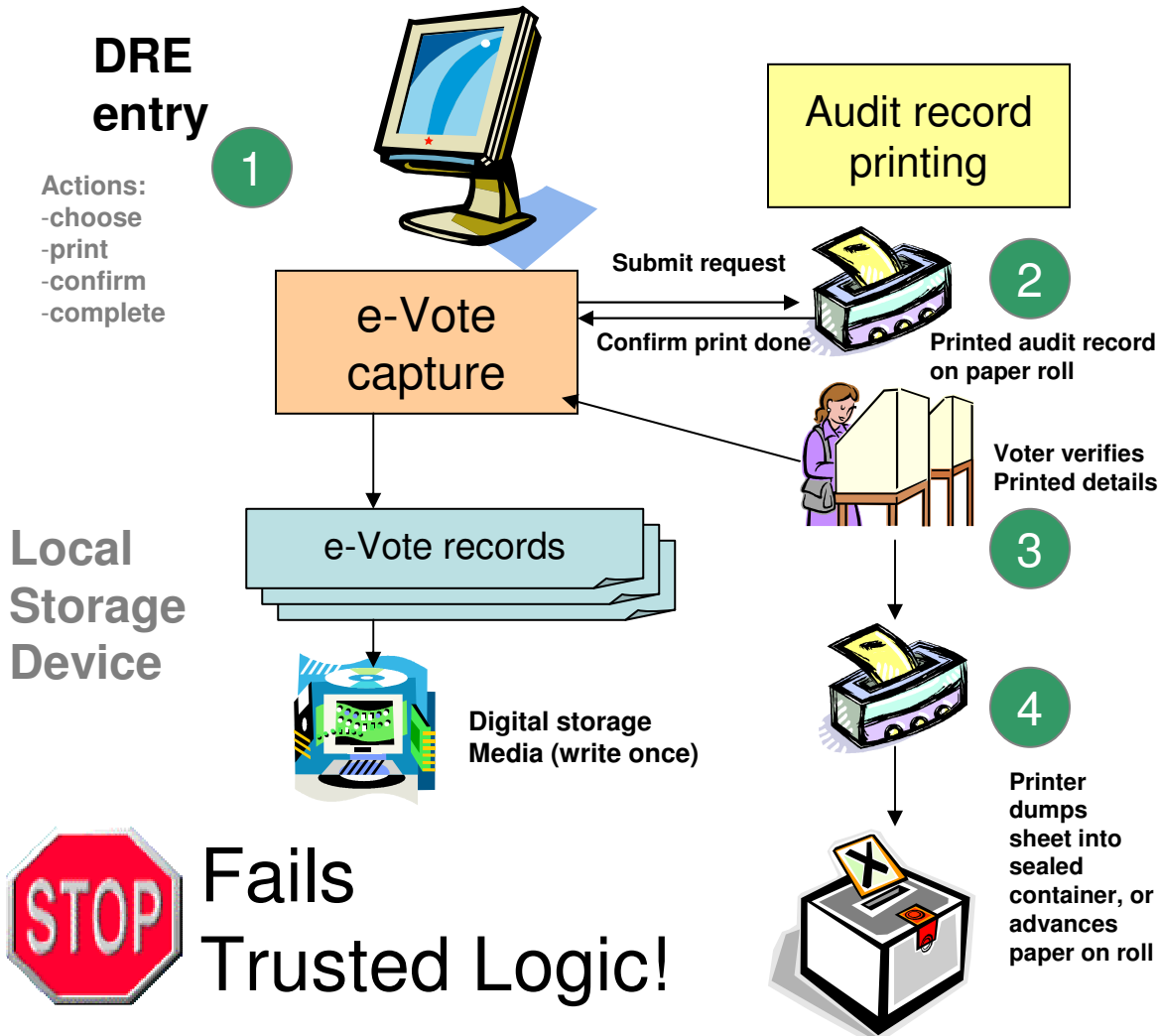
Summary – What EML supports

- Allows implementation of *trusted logic process* combining paper and digital ballots
- Details 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
- Open international public specifications

Useful Resources

- Website of Professor Rebecca Mercuri - <http://www.notablesoftware.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
- 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
- IEEE P1622 - http://grouper.ieee.org/groups/scc38/1622/p1622_documents.htm
- Overview of EML: <http://www.idealliance.org/papers/xml03/slides/spencer/spencer.ppt>
- Technical aspects vote processing: <http://gnosis.cx/publish/voting/privacy-electronic-voting.pdf>
- Trusted Logic Voting: <http://trustedelections.org>

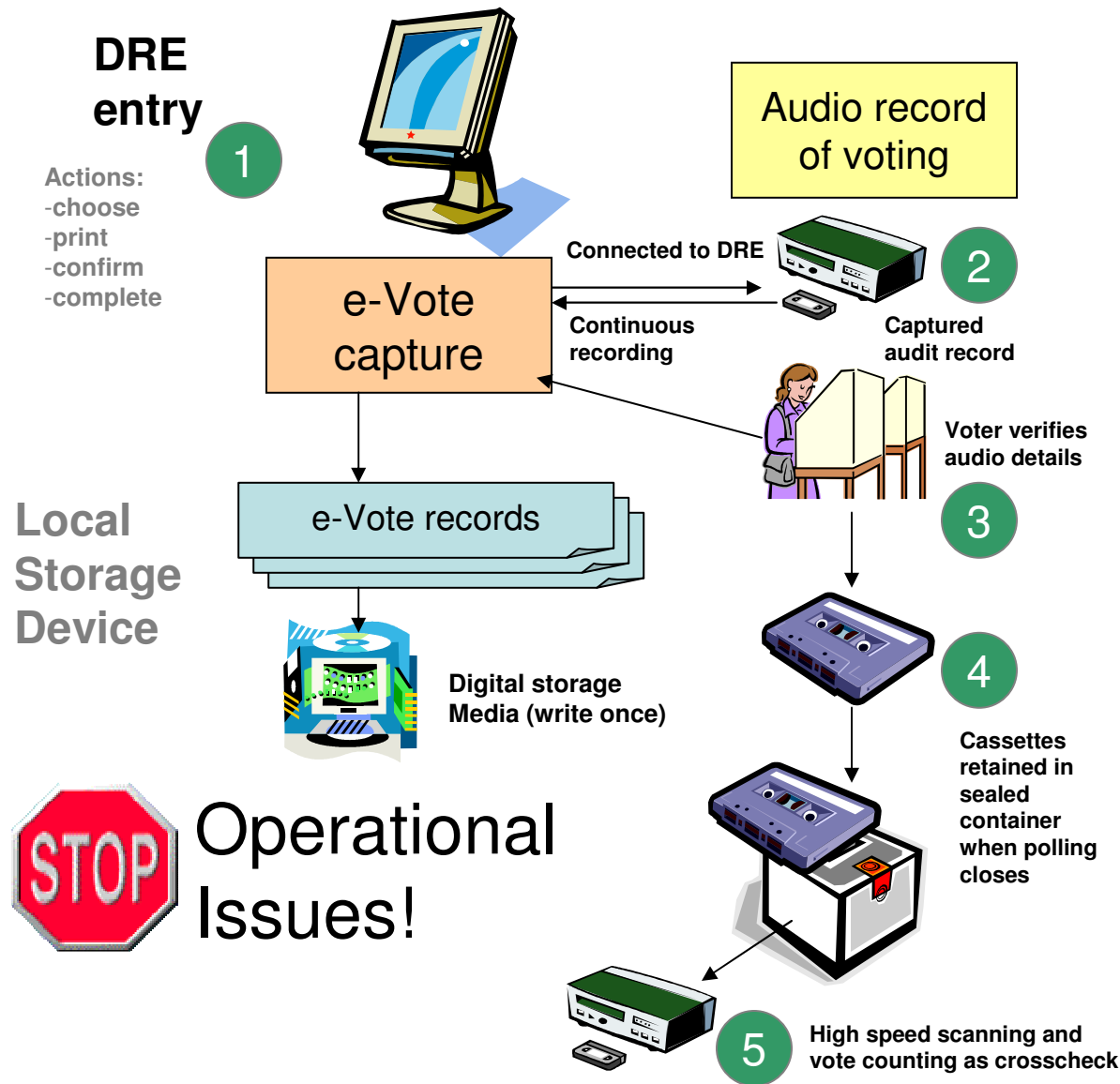
DRE + VVPAT “sealed” Printer Analysis



TRUST ISSUES

- A** Voter unable to directly verify what the printer dumps into the container
- B** Sequence of paper in container may not be random enough compared to single central ballot box
- C** Printer could print information that is not verified by voter (not anonymous)
- D** Single vendor for voting and printing devices
- E** Requires special printer instead of familiar everyday printer
- F** More difficult for visually impaired voters to verify printed ballot behind plexi-glass shield
- G** Equipment reliability and failures
- H** DRE can manipulate vote and printing without needing voter intervention, or by ignoring / misleading voter
- I** Voter cannot be assured that spoiled or incomplete ballots really are ignored
- J** Missing use of standard XML to configure ballot forms and manage printing

DRE + VVPAATT Audio Device Analysis



TRUST ISSUES

- A** Voter unable to directly verify that the recording has taken place
- B** Sequence of recording on cassette can compromise voter privacy
- C** Recording can contain information that is not heard by voter (vote manipulation)
- D** Digital media may be damaged, unusable, or fail to record.
- E** Operation slower than paper-based balloting because of audio dialogue
- F** Deaf voters cannot use the verification system
- G** Manual processing of audio records difficult if by-hand audit required
- H** Equipment reliability and unrecoverable failures leading to potential vote loss
- I** Custody of and changing cassettes when full
- J** Voter cannot be assured that spoiled or incomplete ballots really are ignored
- K** Missing use of standard XML to configure ballot form details and manage audio dialogues (VoiceXML)