6.6: Integratability and Data Export

Voting devices must connect and work with each other without a lot of effort, even if from different vendors

Voting devices must speak (produce records) using a commonly understood language, same format, same grammar

Integratabilty = able to be integrated

- Devices must use common hardware interfaces
  - E.g., USB, RS-232
- Manufacturers should use common industry methods for hardware connections, signaling, protocols

Common Data Export/Interchange

- Goals:
  - All electronic records, regardless of device or vendor, are in the same format and can be read, audited, tabulated with the same sort of software
  - Ballot definition files need be created once, not once per specific device
  - Records from different devices, even vendors, can be easily aggregated

6.6-B: Use non-restrictive public format

- Affects all voting devices
  - DREs, VVPATs, Op scan, EBM
  - EMS
  - Electronic poll books
- Format must be freely publicly-available
- There cannot be restrictions on the use of the format – fees, etc.

6.6-B.4 – Explain the format

- Vendor must fully document the format
  - A jurisdiction should be able to write its own software to interact with vendor-formatted data
  - The vendor must provide a sample program with source code to show how formatted data can be read, etc.

6.6-B.6,B.7: 'should' requirements

- Vendors should use a format common to all of their equipment
- Vendors as a whole should use the same consensus-based format
- Examples include:
  - OASIS EML
  - IEEE P-1622

7.5.1: Voter Credentials and Ballot Activation

- Determining what type of ballot to present to the voter
- Activating the voting system to present that ballot
- New requirements dealing with electronic pollbooks

Terminology

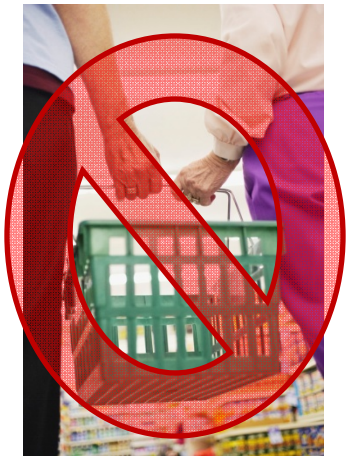
- **Issuance of voter credentials** – what an epollbook or pollworker does
- **Ballot activation** – occurs on a vote-capture device to present the correct ballot style to a voter
- **Activation device** – an epollbook, handheld activator, or other specific device
- **Token** – e.g., a smartcard, holds credentials to build the correct ballot style and enable that voter to cast one ballot
- **Ballot configuration** – the 'raw' set of contests that groups of voters are eligible to vote, included in the credentials
- **Ballot style** – the presentation to a voter of the configuration, with options for alternative languages, ordering of contests, etc.

Credential issuance & ballot activation

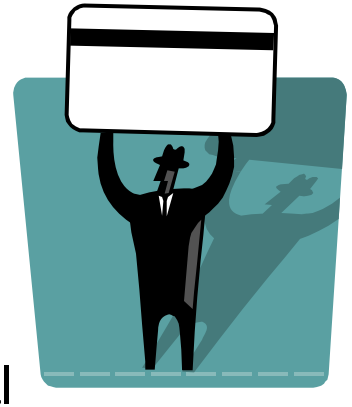
- Requirements for basic aspects of ballot activation and credential issuance
- DRE/EPB can be an activation device but not both at same time
- Can cast at most one ballot
- Activation device controls ballot configuration, e.g., the Democrat contests in a primary
- DRE/EPB reads ballot configuration, enables only those contests for that configuration, e.g., voter's ballot contains only Democrat contests

Secrecy of the ballot

- Secrecy of ballot must be protected at all phases
- Activation device records cannot be combined with other records to identify a ballot
  - Exception made for provisional voting



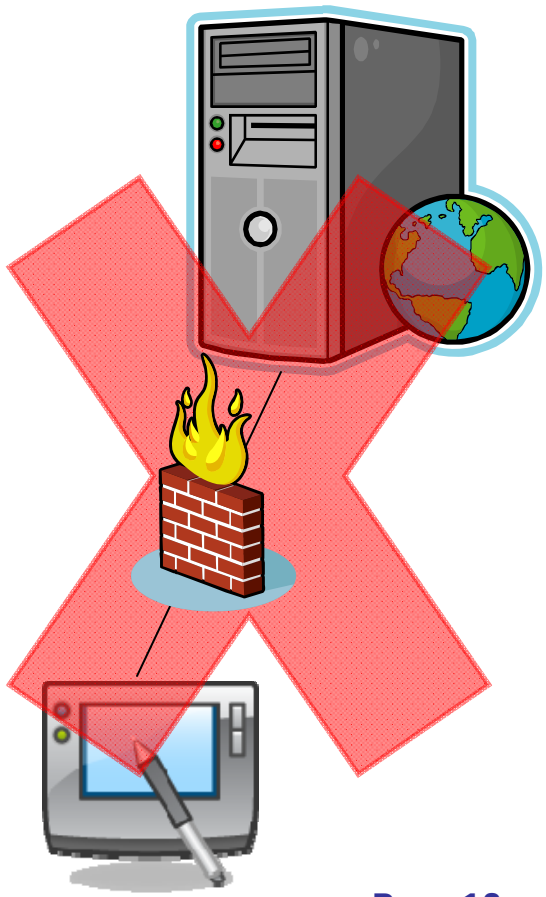
Credentials and Tokens



- Sole purpose is for activating the ballot
- Token should be limited in size to what is needed
- If token re-used, must be cleared first
- Created by an activation device such that...
  - Vote-capture device can verify integrity of credential information
  - Vote-capture device can verify it was created from an authorized activation device
  - Can be done with shared cryptographic keys between vote-capture device and activation device

Connections to remote voter registration DBs

- Much TGDC discussion of this issue
- If the activation device is connected to a remote database, many potential security issues
- TGDC ultimately permitted this, but levied a number of security requirements



Connections to Remote DBs

- Activation device may connect ONLY to access or update a voter registration DB
  - Network access cannot be used otherwise
  - Cannot connect to a network of vote-capture devices AND remote voter registration DB at same time
- Must require authorization to connect, connection must be obvious to pollworker
- Capability for backup if remote connection fails
- Need wired connection to a firewall, no wireless