Organization for the Advancement of Structured Information Standards (OASIS) Comments: VVSG Electronic Records Requirements, 6/12/07

Chapter 5: Electronic Records Requirements

5.1 Introduction/Scope

In order to support auditing, a voting system must be able to produce electronic and paper records that contain the needed information in a secure and usable manner. Section XX defines the general requirements on voting systems to support auditing. This chapter addresses the requirements that specifically relate to electronic records and Section XX address the requirements that specifically relate to paper records.

Electronic records include records produced by any type of voting machine such as DREs, Optical Scan tabulators, or electronic management systems. They typically include records such as:

- Vote counts;
- Counts of ballots recorded;
- Information that identify the electronic record;
- Event logs and other records of important events or details of how the election was run on this machine; or
- Election archive information.

By ensuring that certain reports are produced, secured, and exported, many attacks can be guarded against such as:

- Tampering with electronic records in transit from the polling place to the tabulation center.
- Tampering with the operation of the tabulation center; or
- Altering election records after the totals are determined.

There are two primary types of requirements related to electronic records. The first type addresses what data must be included in the electronic records and the second type addresses securing that data to prevent or detect changes.

The EML Core schema provides definitions of core data elements, e.g. ballot items, counts, names and addresses, that are to be used in the e-voting processes. The core elements can be extended as necessary and localised using Schematron, CAM and/or other validators if specific validation rules are to be applied.

The security of data is handled by the EML Vtoken element and data sealing procedures. This together with the EML Audit Log Schema (480), which has been specifically developed to record and report all activities in the e-voting processes, allows formal tracking of access to and updates of records.

EML also provides a formal minimum information set. It is important to specify not only what should be recorded, but also what should not be recorded. This prevents one part of the voting process compromising a later part by passing malicious or unintended information.

These requirements include those for cryptographically signing electronic records and ensuring that the records are in a publicly-specified format. This chapter specifies requirements on electronic records used to move information about election results between machines within the full voting system, to support required auditing steps, and to report votes to the public.

EML provides a complete record of all the election digital artifacts, from ballots and candidates to votes, counting and reporting. These can be stored to read-only media as a permanent public record of the entire election that can be independently inspected and verified.

5.2 Requirements on Electronic Records and Report

5.2.1 Requirements on All Records Produced by Voting Equipment

The following requirements apply to records produced by the voting system for any exchange of information between machines, support of auditing procedures, or reporting of final results.

□ **5.2.1-A** Records required to be in open format

All electronic records in this chapter ***SHALL*** be produced in a fully specified, public format.
The public standard should be from an accredited standards body, such as OASIS, with an applicable open review process and not just a local government appointed body or private vendor provided format or modifications. The standard should accommodate any legally defined data for the election processes plus open international standards for the other data.
The process should include conformance test suites to ensure that the records adhere to the structure definitions and content models of the publicly published standards. When using XML-based record structures like EML, then tools such as Schematron and OASIS CAM can provide strong content checking and conformance tests.

Applies to: Voting Device
Test Reference:
DISCUSSION
Requiring all electronic records to appear in a public format ensures that election officials can read and review the contents of the records with software not provided by the voting system vendor. This permits auditors to get review the data in the records without the need to trust software provided by the vendor.
Using open formats such as W3C XML ensures that records are in a plain and open syntax for which there are huge arrays of available open public tools that can inspect and display the content of the voting digital artifacts. In addition EML can be reviewed and displayed by any XML compatible tool without requiring special code or plug-ins.

Source:
Impact:

□ **5.2.1-B** Records to be capable of being printed

The voting system software ***SHALL*** provide the ability to produce printed forms of all records in this chapter. The printed forms ***SHALL*** retain all required information as specified for each record type.
All data handled by EML XML schema record types can be sent to specified printers or other output or visual display devices for direct rendering “as is”. In addition specified reports using any type of style sheets can be defined in the EML Structure linkage provided in each schema – so that bespoke human friendly presentation can be made directly from the XML record content.

Applies to: Voting Device
Test Reference:
DISCUSSION
Printed versions of all records in this chapter are either necessary or extremely helpful to support required auditing steps, as specified in the Auditing chapter.
EML XML records can be stored into appropriate database systems after conclusion of the elections, and provide additional post-analysis and audit support through queries and crosscheck independent computations and statistical analysis.

Source:
Impact:

Electronic Records Requirements

5.2.2 Requirements on Records Produced by Voting Machines and Scanners

The following requirements apply to records produced by voting machines and scanners for exchange of information between machines, transmission of results to a central tabulation center, support of auditing procedures, or reporting of intermediate election results.

□ **5.2.2-A** Cryptographic Protection of Records from Voting Machines

All electronic records from voting machines in this chapter ***SHALL*** be digitally signed with the Election Signature Key, and ***SHALL*** include a certificate linking the records to the source machine's long-term signing key and ID.

This requirement can be met by use of the Seal element provided in the EML schemas.

Applies to: Voting Device
Test Reference:
DISCUSSION
The Cryptography chapter specifies the production of the Election Signature Key (ESK), a per-election signing key; these keys are used to sign records from a single election. The Election Public Key Certificate links the per-election signing keys to a permanent per-machine signing key, and a unique identification of the machine which generated the key and the record. The digital signatures address the threat that the records might be tampered with in transit or in storage. The certificate linking each record to a machine addresses the threat that a legitimate electronic record might be misinterpreted as coming from the wrong voting machine or scanner. The use of per-election keys to sign these records addresses the threat that a compromise of a voting machine before or after election day might permit production of a false set of records for the election, which could then be reported to the tabulation center.
Source:
Impact:

□ **5.2.2-B** Requirement to Verify Signed Records

The tabulation center ***SHALL*** verify the correct receipt of electronic records from voting machines and scanners. For each voting machine which produces electronic records according to this standard, the tabulation center ***SHALL*** verify that the election ID, timestamp, and digital signature are correct before accepting the record.

This requirement can be met by use of EML schema 480 in addition to the Vtoken support in each individual ballot record such in EML 440 ballot records.

Applies to: Click here to add the Applies to text
Test Reference: Click here to add the Test Reference
DISCUSSION
The digital signature applied to the electronic records from the voting machines is only useful if it is verified before the tabulation center accepts electronic records.
Source:
Impact:

□ **5.2.2-C** Electronic records poll opening certificate requirement

Upon opening the polls, the voting machine ***SHALL*** produce an Election Public Key Certificate to include the following information:

This requirement can be met by use of EML schema 340 and specifically datatypes PollingPlaceStructure and ProcessingUnitStructure. Provision is also made for handling the recording of software versions as needed.

♦ Date and time at which the polls opened initially for the election.
♦ Serial number and other identifying information of the voting system and cryptographic module.
♦ Precinct and list of ballot styles supported, including hashes of each ballot definition.
♦ Hardware-enforced counter, which is immediately incremented upon being used
♦ Current version of software on the voting system.
♦ Election Signature Key key.
♦ Digital signature with Device Signature Key of the cryptographic module.

Applies to: Click here to add the Applies to text
Test Reference: Click here to add the Test Reference
DISCUSSION
This record exists to strongly bind together the ESK, a per-election key, an initial poll opening time and date, a precinct and set of ballots, and a voting system. The record can be used along with associated records to make sure that each voting system that is supposed to send in some votes get to send in exactly one set of ballots, and that no additional sets of ballots are supported. The record also makes it possible to determine that all the electronic records originated from this voting system. The record can be used to verify that the voting system had the correct set of ballot definitions and styles loaded at the time of the election, and the correct version of software. The inclusion of the counter in this certificate makes it possible to detect any spurious generations of per-election keys, such as might have occurred in the past to attempt to alter another election total. This record is used in combination with others to resist a number of attacks, including attempts to insert additional or altered electronic records into the total. See the Cryptography chapter for more details on the requirements for generating and destroying per-election keys.
In addition to hardware mechanisms for unique counters, paper records with unique sequence bar code values are equivalent. Those bar code values are also coded and can be stored in the EML ballot identification to provide direct correspondence between paper records and digital ones. The coding sequences can be assigned to particular polling places and ensure only those ballots are counted, and only once.

Source: Click here to add the Source
Impact: Click here to add the Impact

□ **5.2.2-C.1** Electronic records poll opening certificate handling requirement
The voting machine ***SHALL*** handle the Election Signature Certificate according to the following:
This requirement can be met by use of EML schema 340 as mentioned above.

♦ The certificate is transmitted to the tabulation center with the other electronic records.
♦ It is stored in the election archive, if available.
♦ It is written to the voting systems event log.
♦ If a printer is available, it should be printed in a format that allows it to be scanned back into a valid certificate.
Applies to: Click here to add the Applies to text
Test Reference: Click here to add the Test Reference
DISCUSSION
Click here and type the discussion about this requirement
Source: Click here to add the Source
Impact: Click here to add the Impact

□ **5.2.2-D** Electronic records poll closing records requirement

Upon closing the polls, the voting machine ***SHALL*** produce a report including the following records:

This requirement can be met by use of EML schemas 460 and 470.

♦ Election Signature Key and certificate.

♦ Time and date when the report was generated.

♦ Sufficient information to allow counting of the votes. This may be vote counts or ballot images, depending on the system.

♦ A digital signature from the Election Signature Key.

Applies to: Click here to add the Applies to text

Test Reference: Click here to add the Test Reference

DISCUSSION

This record exists to carry the results from the voting system back to the tabulation center, where it can be combined with the results from other voting systems to determine a winner in each race. The tabulation center can verify the signatures in both the per-election key and certificate and in this record before accepting the data into the total. This record is sufficient to support random recount audits of paper records. It can be used to verify a correct result from a system under parallel testing. This record can be used to randomly check electronic totals, when the final result is given broken out by voting system or scanner. By requiring inclusion of the per-election key and certificate, and by signing the whole record, this electronic record format entirely eliminates attacks that rely on tampering with electronic records in transit. Because the per-election key is destroyed soon after writing this record, there is no way for an attacker to backdate electronic records when an audit or recount is called for. See the Cryptography chapter for more details on the requirements for generating and destroying Election Signature Keys.

Source: Click here to add the Source

Impact: Click here to add the Impact

□ **5.2.2-D.1** Electronic records poll closing records handling requirement

The voting machine ***SHALL*** handle the poll closing records according to the following:

This requirement can be met by use of EML schemas 460 and 470.

♦ The records are transmitted to the tabulation center with the other electronic records.

♦ It is stored in the election archive, if available.

♦ Its signature is stored in the voting systems event log.

Applies to: Click here to add the Applies to text

Test Reference: Click here to add the Test Reference

DISCUSSION

Click here and type the discussion about this requirement

Source: Click here to add the Source

Impact: Click here to add the Impact

□ **5.2.2-E** Electronic records summary count record requirement

The voting machine ***SHALL*** produce a summary count report including the following:

This requirement can be met by use of EML schema 510.

♦ Election Signature Key and certificate

♦ Time and date at poll closing

♦ List of ballot styles voted and for each style, how many ballots are stored.

♦ Number of spoiled ballots, if any.

♦ Ballots not yet properly counted (i.e. provisional ballots)

♦ For each ballot question:

♦ Number of ballots voted that included the question

♦ Number of votes for each candidate for this question

♦ Number of votes for some write-in for this question

♦ Digital signature

Applies to: Click here to add the Applies to text

Test Reference: Click here to add the Test Reference

DISCUSSION

The summary count record gives a summary of the results of voting on this voting system of scanner, the result of the election that would result if only this voting system's votes were counted. This summary is preliminary because provisional ballots and write-in votes may be included in the records stored by the voting system, but may not yet be able to be counted. This record can be printed (with digital signatures encoded into printable characters) and can also be stored electronically. This record exists to allow checking of the final totals, based on their agreement with local totals from the voting systems, without the need to entirely trust the computers and workers at the tabulation center. For voting systems that send a set of ballot images to the tabulation centers, this summary should in general be safe to publish, whereas the set of ballot images is not safe to publish. This record is not complete because provisional and write-in ballots require human intervention to count. However, the set of all such records will yield an approximate election result. This record does not provide much security benefit when used with instant runoff voting (IRV). This record is sufficient to support random recount audits of paper records. It can be used to verify a correct result from a system under parallel testing. This record can be used to randomly check electronic totals, when the final results are given broken out by voting system or scanner. It can be published for each voting system, along with corrected final totals for each precinct and for absentee ballots, to show how the final election outcomes were computed. When published for each voting system and included in a summary of final election outcomes, this record blocks the class of attacks that involves tampering with the tabulation center computer. It provides an auditing process in which the records can be used by election official and observers to catch any misbehavior in the tabulation center with high probability. A further safeguard can be provided by EML using the schema 410 ballot layout image and ID references to create counting records resistant to attacks involving exposed plain text party and other affiliation information. The interim schema 510 totals therefore reflect only those 410 reference ID values, and only the schema 520 election results fully expose all party and affiliation information. Those schema 410 ballot layout images would be excluded from all computer systems except the one secure central election result reporting system. This prevents the counting software and the local voting software from knowing plain text information about the ballot choices and election outcomes.

Source: Click here to add the Source

Impact: Click here to add the Impact

□ **5.2.2-E.1** Electronic records summary count record handling requirement

The voting machine ***SHALL*** handle the summary count record according to the following:

This requirement can be met by use of EML schema 510.

♦ The record is transmitted to the tabulation center with the other electronic records.

♦ It is stored in the election archive, if available.

♦ It is stored in the voting systems event log.

Applies to: Click here to add the Applies to text

Test Reference: Click here to add the Test Reference

DISCUSSION

Click here and type the discussion about this requirement

Source: Click here to add the Source

Impact: Click here to add the Impact

□ **5.2.2-F** Collection of cast vote records requirement

The voting machine ***SHALL*** produce a collection of cast votes recorded, including the following election:

This requirement can be met by use of EML schemas 440 and 460.

- Election Signature Key and certificate
- Time and date at poll closing
- The set of cast vote records recorded from this election by this voting machine, in randomized order. For each vote, this includes:
- Precinct, election district, and ballot style
- The vote as recorded on each ballot question
- Undervotes as recorded on each ballot question
- Write-in information as recorded on each ballot question
- Information specifying whether the ballot is provisional, and providing identifying information if so.
- Digital signature

Applies to: Click here to add the Applies to text
Test Reference: Click here to add the Test Reference

DISCUSSION

The collection of cast vote records contains the full set of votes that were recorded by the machine. This is required to support instant runoff voting, and is extremely useful in investigating possible problems in an election.

Source: Click here to add the Source
Impact: Click here to add the Impact

□ **5.2.2-F.1** Collection of cast votes handling requirement

The voting machine ***SHALL*** handle the collection of cast votes record according to the following:
This requirement can be met by use of EML schema 460.

- The record is transmitted to the tabulation center with the other electronic records.
- It is stored in the election archive, if available.
- It is stored in the voting systems event log.

Applies to: Click here to add the Applies to text
Test Reference: Click here to add the Test Reference

DISCUSSION

Click here and type the discussion about this requirement

Source: Click here to add the Source
Impact: Click here to add the Impact

□ **5.2.2-G** Electronic records event log report requirement

The voting machine ***SHALL*** produce an event log report with the following information:
This requirement can be met by use of EML schema 480.

- Election Signature Key and certificate
- Event log data from poll opening until poll close
- Signature

Applies to: Click here to add the Applies to text
Test Reference: Click here to add the Test Reference

DISCUSSION

Event log formats and requirements are specified in the System Integrity Management and System Event Logging chapters. The event log contains a listing of security-relevant events (such as installation of new software) and procedure relevant events (such as the opening of the polls). The purpose of event logs is to leave a permanent trail of anomalies and misbehavior, so that these may be discovered later. Event logs must not include sufficient information to reconstruct the order of votes or to determine how any voter voted. The event logs support detection of problems by both manual and automated scanning. They also support investigation of any problems discovered. Event logs cannot rule out software tampering and related attacks, but

make them more difficult to carry out without detection. Event logs can detect failure to follow procedures and even some lowtech attacks by pollworkers.
Source: Click here to add the Source
Impact: Click here to add the Impact

□ **5.2.2-G.1** Electronic records event log record handling requirement
The voting machine ***SHALL*** handle the event log record according to the following:
This requirement can be met by use of EML schema 480.

♦ The record is transmitted to the tabulation center with the other electronic records.
♦ It is retained on the voting system.
Applies to: Click here to add the Applies to text
Test Reference: Click here to add the Test Reference
DISCUSSION
The tabulation center can verify that the event log record is received and that the digital signature and per election key and certificate are valid.
Source: Click here to add the Source
Impact: Click here to add the Impact

5.2.3 Requirements on Records Produced by Tabulation Center Computers

The following requirements apply to the final election tally produced by the tabulation center computers and released to the public.

□ **5.2.3-A** Final election tally report requirement

The tabulation center voting machine ***SHALL*** produce a final election tally report.
This requirement can be met by use of EML schema 520.

The report ***SHALL*** contain the following information:

♦ The election totals

♦ The total number of ballots, and ballots of each style, precinct, and election district

♦ For each polling place:

♦ The serial numbers and public keys for each voting system used in the precinct. In the case of older equipment that doesn't support the use of per-election public keys, the serial number ***SHALL*** be included.

♦ The Summary Count Record for each voting system used in the precinct. In the case of older equipment that doesn't support the Summary Count Record, the same summary information is included, but without the digital signature, timestamp, and per election key and certificate.

♦ Any adjustments done to the precinct or polling place counts due to provisional ballots, write-ins, and other special cases.

♦ A digital signature

Applies to: Click here to add the Applies to text
Test Reference: Click here to add the Test Reference

DISCUSSION

The tabulation center record exists to allow checking of the final totals, based on their agreement with local totals from the voting systems, without the need to entirely trust the computers and workers at the tabulation center. The goal is to provide cryptographic support for a process that is currently done in a manual, procedural way, which may be subject to undetected error or tampering. This is the best record to use to support random recount audits of paper ballots and VVPAT records, since it includes resolutions for the special cases at the polling place level to preserve ballot secrecy for provisional ballots. This record can be published for each voting system, along with corrected final totals for each precinct and for absentee ballots, to show how the final election outcomes were computed. Challenges to handling of special cases per precinct can be made and checked base on this record. This report blocks most misbehavior at the tabulation center.
In addition EML supports by use of the schema 410 ballot layout to automatically and externally drive the generation of the EML schema 510 counts and EML schema 520 report without requiring programmers to explicitly internally hard code counting totals and plain text array inside their software. This permits election officials to independently control the ballot setup, counting and reporting operations without involving coding by programming staff. This is especially important for open public voting implementations that use community developed software as opposed to private proprietary software.

Source: Click here to add the Source
Impact: Click here to add the Impact

□ **5.2.3-B** Election tally audit report requirement

The tabulation center voting machine ***SHALL*** be capable of producing a report from the election tally which supports auditing requirements.
This requirement can be met by use of EML schema 510.

The report ***SHALL*** contain the following information:

- The election totals
- The total number of ballots, and ballots of each style, precinct, and election district
- For each polling place:
    - The serial numbers and public keys for each voting machine or scanner used in the polling place. In the case of older equipment that doesn’t support the use of per-election public keys, the serial number ***SHALL*** be included.
    - The final summary of votes from that voting machine or scanner, including resolved write-in votes, and indications of provisional ballots that should and should not be included in the totals.
- A digital signature

Applies to: Click here to add the Applies to text

Test Reference: Click here to add the Test Reference

DISCUSSION

This report supports hand-auditing of paper records against the final totals, and includes the resolution of provisional and write-in votes. This report could leak information about how some provisional ballots voted, but also provides more complete information for auditors to check against voter-verifiable paper records.

Source: Click here to add the Source

Impact: Click here to add the Impact