

NOTICE

The following document contains professional opinions and expert judgment that would be unsuitable for some audiences. Viewer discretion is advised.

On device-level certification and interoperability

Developmental work

2008-03-07 17:31

1 Introduction

In a letter dated 2008-02-13, the EAC requested NIST's assistance in:

...Developing a feasibility study of the ramifications of the EAC separately testing and certifying components of a voting system, and requirements for interoperability between systems and system components. In addressing this, the EAC would ask NIST to address the feasibility of requiring, in the next iteration of the VVSG, a specific standard for the format of electronic election data and the inclusion of requirements for standard methods for exporting electronic election data. [1]

We find four separate questions in this request.

[Section 2](#): What are the ramifications of separately testing and certifying voting devices?

[Section 3](#): What would a requirement for interoperability look like?

[Section 4](#): What is the feasibility of requiring, in the next iteration of the VVSG, a specific standard for the format of electronic election data?

[Section 5](#): What is the feasibility of requiring, in the next iteration of the VVSG, standard methods for exporting electronic election data?

2 Ramifications of device-level testing and certification

2.1 Prescribed architecture

In order for certification of a device to have any practical meaning, it is necessary to have some idea of how that device integrates with others and what its functions and responsibilities within the voting system are. In other words, we need to know the architecture of the voting system.

The public review draft of the VVSG does not specify an architectural model because it would constitute an unnecessary design requirement. Manufacturers are currently free to invent new ways of satisfying the requirements of the voting process using new kinds and combinations of devices. There was no reason to restrict that freedom until the issue of device-level certification arose.

It would be feasible to add an architectural model for voting systems to the next VVSG. However, since a system or device whose architecture could not be mapped onto that standard architecture might become uncertifiable, it would discourage innovation.

2.2 No assurance of system-level conformance

To infer that a voting system is conformant based only on the conformance of its devices is an instance of the fallacy of composition [2].

To draw valid conclusions about the system as a whole based on facts about its parts, one needs not only an analysis of the parts but also a valid model of how the system-level behavior logically follows from the device-level behavior. For example, if one considers reliability in isolation from other concerns, one can perform a fault tree analysis (FTA) [3] and/or a failure mode, effects, and criticality analysis (FMECA) [4]. Similar principles are used in the logic verification discussed in the draft VVSG [5].

Unfortunately, voting system conformance has many dimensions—accessibility, usability, privacy, secrecy, auditability, etc.—and most of these dimensions do not have anything analogous to a fault tree analysis that one can perform. Some high-level properties are holistic and have no logical connection to low-level properties at all. Thus we conclude that a valid, general model relating voting system conformance to the conformance of its constituent devices is probably infeasible even if an architecture were prescribed (see Section 2.1).

In the best possible world—assuming that all of the subtle -ilities could be handled with something analogous to a fault tree analysis—the analysis would be complex, requiring specialized expertise, and would not necessarily save time or money relative to complete system testing (which ought to be done anyway to validate the analysis).

3 A requirement for interoperability

A requirement saying simply *voting devices shall be interoperable* would be well-intentioned but ill-formed. Interoperability is an attribute not of a device, but of the relationship between two or more devices. One cannot meaningfully say that a device is interoperable without answering the question *with what?*

In practice, the intent of the above requirement must be separated into two synergistic concerns: conformance to data format and interface standards, and demonstrated interoperability with one or more products from other manufacturers. This truth and its consequences are explored in more detail in the following subsections.

3.1 Relevance of standards to interoperability

Conformance to a standard is neither necessary nor sufficient to achieve interoperability. It is unnecessary because interoperability can be achieved with *ad hoc* interfaces. It is insufficient because it is always possible to construct an integration scenario in which a failure will occur because of some property that was not explicitly modelled in the standard [6].

The value of conformance to data format and interface standards is not in providing a guarantee of interoperability for devices that have never before been integrated, but in reducing the cost of performing that integration. Greater commonality in the data elements and interfaces implemented by the devices usually means a lower integration cost. In the best possible case, it could, in theory, be zero (i.e., works first time).

However, even with conformance to the same data format and interface, a successful integration is by no means assured. A wide variety of technical, semantic, functional, policy, and logistical conflicts can arise when integration is attempted (see [7, Section 5, Integration concerns]). Such conflicts are occasionally alleged to have been engineered deliberately to sabotage interoperability with competing products (e.g., [8, ¶102–114]).

The feasibility of requiring specific data format and interface standards in the VVSG is explored in [Section 4](#) and [Section 5](#) respectively.

3.2 Interoperability testing

Since interoperability is an attribute of the relationship between two or more devices, conformance testing of a device by itself reveals little about interoperability. Instead, interoperability testing must be conducted with all of the devices that are intended to work together. Interoperability testing consists of bringing together existing products, configuring them to work together, and performing an operational test to determine whether they are in fact capable of working together.

Manufacturers of products that implement networking and data communications protocols have historically achieved and maintained interoperability through voluntary, manufacturer-driven interoperability testing events known as plugfests. Manufacturers get their products to work with the products of whichever other manufacturers show up for the plugfest. Plugfests are held periodically to ensure that interoperability is maintained as products evolve and new products appear. The University of New Hampshire’s InterOperability Laboratory currently hosts plugfests for implementors of many different networking and data communications protocols [9].

The plugfest approach is often imitated outside of the networking and data communications specialty. Levels of success vary, with manufacturer commitment to achieving real interoperability being the most critical success factor. When that commitment is lacking, the testing focus of plugfests tends to be replaced with a marketing focus. The interoperability *test*, in which manufacturers try to discover and correct faults in their products, is usurped by an interoperability *demonstration*, in which manufacturers try to avoid reproducing known faults or discovering new ones (thus eliminating any possible value that the event would have in achieving or maintaining interoperability).

If interoperability testing were to be driven by mandate rather than voluntary manufacturer commitment, the authority issuing the mandate would be obliged either to choose the specific products with which interoperability must be demonstrated (unavoidably granting a competitive advantage to those products) or to define a process through which that choice would be made. The corresponding VVSG product requirements would then be of the form either *voting devices shall interoperate with X, Y and Z* or *voting devices shall interoperate with the pool of reference implementations determined by process P*, and interoperability testing would be specified as the test method. There would need to be a collection of such requirements to mandate interoperability across each interface in the standard architecture (see [Section 2.1](#)).

4 Feasibility of standard data format in the next VVSG

We believe that any data format mandated by the VVSG should meet the following conditions:

1. It should support all of the voting variations defined in the VVSG.
2. It should have a coherent data model with strong conceptual integrity.
3. It should be vetted by U.S. voting system manufacturers to ensure that it contains no critical errors or omissions.
4. In the spirit of HAVA §221 (42 U.S.C. 15361) (e)(3) [10], it should be unencumbered by any copyrights, patents, or trade secrets that would oblige VVSG implementors to pay royalties to or sign agreements with intellectual property owners.

Unfortunately, we are unaware of any existing candidate standard that satisfies or is near to satisfying those conditions. To specify a standard data format in the next VVSG, it would be necessary either to compromise on the above conditions or to make VVSG finalization dependent on the successful completion of a lengthy process of standards development and/or revision.

4.1 Election Markup Language (EML)

Election Markup Language (EML) [11] is often cited as the only living standard for election data exchange. However, it appears that EML has been damaged by a period of destructive maintenance that has compromised its conceptual integrity.

In late 2006 and early 2007, NIST contacted the chair of the Election and Voter Services Technical Committee of the Organization for the Advancement of Structured Information Standards (OASIS), which controls EML, with questions and issues regarding support for requirements of the VVSG. Our questions and issues were routed directly to the maintainer, who considers most of them to have been resolved in version 5. However, the resolutions to our issues were surprising and largely unsatisfactory, as they exacerbated the conceptual integrity problems that already existed in version 4. Rather than correct previous design errors, the maintainer's preference was to add more data elements or reinterpret existing data elements as a workaround. His advice was then to ignore any data elements that conflicted with the workarounds, even if the standard identified them as being mandatory:

No change. Assume if they are simply made empty tags—this is not harmful—will pass XSD validation but null value associated with them. [12]

The result was a confusing collection of semi-redundant data elements with no single, coherent, normative interpretation.

NIST avoided making public comments against EML as it only would have attracted negative publicity to all involved. But Paul Spencer, who authored schemas for earlier versions of EML, echoed our concerns in his “EML v6 Wish List:”

EML is suffering badly from the effects of its continued evolution. I suggest we build a proper data model to help with the consistency of implementations and provide a better foundation for future change. [13]

In summary, while a voting system integration effort could doubtless be made to succeed using a language derived from EML v5, it would be wiser to begin such an effort with a language or data model whose conceptual integrity was intact. Some earlier version of EML might be a viable starting point, but further investigation would be needed to verify this and to determine how much new material would need to be invented to support the requirements of the VVSG.

4.2 IEEE P1622

Institute of Electrical and Electronics Engineers (IEEE) Project 1622, Voting Systems Electronic Data Interchange [14], was chartered to develop electronic data interchange formats for use by voting devices. It produced a draft standard in which concepts from an unpublished schema developed by the Open Voting Consortium (OVC)¹ [15] were mapped into EML (see Section 4.1) and EDX (see below). The draft standard remains unpublished and unavailable to the general public.

EDX (acronym expansion unknown) is a specification that Hart InterCivic promulgated as a candidate for standardization. Hart indicated informally that it would waive its copyright over EDX if EDX were adopted as part of IEEE P1622. Failing that, EDX remains the intellectual property of Hart InterCivic.

The P1622 draft went to ballot in March 2007, but the balloting process was aborted to make way for a reorganization of the parent committee (Standards Coordinating Committee 38 [16]). There has been no activity in P1622 since then (as of 2008-03-07). The parent committee has not yet completed revisions to its policies and procedures, but there has been activity there. Thus, while Project 1622 remains officially alive, it has been in limbo for a year, and is difficult to project the likelihood or time frame in which IEEE might approve a P1622 standard.

Since the P1622 draft does not specify an independent data format, the most significant impact of its approval would be for EDX possibly to become available and usable as an alternative to EML. However, unless some special arrangement were made, users would need to purchase a copy of the P1622 standard to obtain access to the EDX schema. IEEE normally asserts full copyright over its standards and prohibits free copying [17].

4.3 Other

Various projects in academia and even at NIST have developed data models that could serve as the basis for an election data format standard. However, the process of evolving such a model into a credible data format standard and then vetting that standard with manufacturers and other stakeholders would essentially be yet another standardization effort facing the same hazards as previous attempts. Given sufficient time, resources, and political capital, it is possible that a standard tailored to the goals of the EAC could be developed, but it is unlikely that consensus for another standard could be built in a time scale that would fit within the planned release of the next VVSG. Prior commitments to EML or proprietary data formats might prevent any public support for another standard from emerging.

5 Feasibility of standard data export method in the next VVSG

Mandating a data export method is relatively uncomplicated. For example, see 47 CFR 76.640 [18], requiring digital cable systems to include a functional home digital network interface. However, as was discussed in Section 3.1, conformance to an interface standard in and of itself is insufficient to yield interoperability, and it does not necessarily empower end users to achieve their integration goals.

¹Kurt Hyde, the vice-chair of the P1622 working group, was a founding member of OVC.

Like all design requirements, a mandatory data export method would live on borrowed time with respect to the regular and rapid “churn” of information technology. There is a significant risk that the equipment or software necessary to use the mandated interface might become obsolete before the next VVSG is finalized, and quite high probability that it would do so before the anticipated retirement of voting systems certified to the next VVSG.

6 Conclusion

Many aspects of the EAC’s request are technically feasible to implement. However, they are unlikely to achieve the goal of voting device interoperability unless they are complemented by periodic interoperability testing.

References

- [1] Brian Hancock. Letter to Mark Skall, February 13, 2008.
- [2] Gary N. Curtis. Logical fallacy: Composition. In *Fallacy Files*. <http://www.fallacyfiles.org/composit.html>, 2008.
- [3] David F. Haasl, Norman H. Roberts, William E. Vesely, and Francine F. Goldberg. Fault tree handbook. Staff Report NUREG-0492, U.S. Nuclear Regulatory Commission, <http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0492/>, January 1981.
- [4] Procedures for performing a failure mode, effects and criticality analysis. Military Standard MIL-STD-1629A, November 24, 1980.
- [5] Election Assistance Commission. *Voluntary Voting System Guidelines Recommendations to the Election Assistance Commission*, August 31, 2007. <http://vote.nist.gov/vvsg-report.htm>.
- [6] David Flater. A logical model of conceptual integrity in data integration. *Journal of Research of the National Institute of Standards and Technology*, 108(5):395–402, September-October 2003. <http://nvl.nist.gov/pub/nistpubs/jres/108/5/j85fla.pdf>.
- [7] Edward J. Barkmeyer, Allison Barnard Feeney, Peter Denno, David W. Flater, Donald E. Libes, Michelle Potts Steves, and Evan K. Wallace. Concepts for automating systems integration. NISTIR 6928, National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899, 2003.
- [8] Avadis Tevanian, Jr. Direct testimony. In *United States v. Microsoft*, October 12, 1998. <http://www.usdoj.gov/atr/cases/f2000/2010.htm#20>.
- [9] Group testing/plugfests at UNH-IOL, 2008. <http://www.iol.unh.edu/services/grouptest.php>.
- [10] Help America Vote Act of 2002. Public Law 107-252, October 29, 2002.
- [11] Organization for the Advancement of Structured Information Standards (OASIS). Election Markup Language (EML) v5, December 2007. <http://www.oasis-open.org/specs/index.php#em15.0>.

- [12] David R. R. Webber. RE: Fw: EML 4 issues. E-mail, February 13, 2007.
- [13] Paul Spencer. Develop a data model to support EML. In *EML v6 Wish List*, rev. 1, July 5, 2007. OASIS Election and Voter Services Technical Committee document #24547.
- [14] IEEE Project 1622 home page (inactive), 2007. <http://grouper.ieee.org/groups/scc38/1622/index.htm>.
- [15] Open Voting Consortium home page, 2008. <http://www.openvotingconsortium.org/>.
- [16] IEEE Standards Coordinating Committee 38 (SCC 38) home page, 2007. <http://grouper.ieee.org/groups/scc38/>.
- [17] IEEE Standards Association. Frequently asked questions: Copyright and permissions, patents and trademarks, 2007. <http://standards.ieee.org/faqs/copyrightFAQ.html>.
- [18] Support for unidirectional digital cable products on digital cable systems. 47 CFR 76.640, October 1, 2007. <http://www.gpoaccess.gov/cfr/>.