THE ENGINEER'S GUIDE TO
WORLDWIDE REGULATORY
COMPLIANCE
www.conformity.com

Volume 12, Issue 5
May 2007

Conformity®

ESD Standards:
An Annual Progress Report

Emerging Issues in Standards
An Overview of Automotive EMC Standards

Challenges in Testing
Certification of Voting Equipment in the United States

Design Fundamentals
Shielding Issues for Medical Products

Focus On...
EMI Shielding

Conformity Magazine
531 King Street, Suite 6
Littleton, MA 01460
CHANGE SERVICE REQUESTED

© Photographer: Peterfactors | Agency: Dreamstime.com

Certification of Voting Equipment in the United States

A Distributed and Coordinated Conformity Assessment System

by Stephen Berger

This article will explore the way voting systems are certified in the United States and the safeguards. The 2000 presidential election raised widespread concern about the reliability of punch card voting systems. Since then, the concern has been spread to all electronic voting systems. However, while there is a popular perception that election risk is concentrated in the new electronic voting systems, in fact, comparable risks exist for all voting systems. Mistakes, inaccuracies and malfeasance has always existed. It is the ongoing task of election officials to continually reduce those risks.

To truly improve the election system, the entire system must be dealt with. Everything from voter registration to the final canvas and declaration of the result must be protected, audited and demonstrated to be secure and accurate.

Sadly, almost all of the media attention and an overwhelming portion of scholarly attention has focused on isolated components. Urgent demands are made to improve a single component or function with no attention to the effect on total system security or accuracy. As has been repeatedly demonstrated by changes (often mandated by legislation) since the 2000 election, the end result of well-intended reforms that do not take a system view consistently produce unintended consequences that typically reduce rather than improve the election system. A very specific failure of academic research has been the almost complete focus given the security of the vote in contrast to the overall system and the accuracy of the final decision in an election. What good comes from having completely secure votes if those votes are either illegal to begin with or, alternately, never make it into the final tally?

In contrast to an isolated component focused approach to elections, this article will discuss the certification system and the larger and distributed conformity assessment system for voting systems in the U.S. Lead by the U.S. Election Assistance Commission (EAC) in close partnership with the National Association of State Election Directors (NASED), the ultimate goal of this assessment system is that voting systems meet requirements when used in elections. While demonstration of compliance in a laboratory is helpful, it is compliance with those same requirements during use that is the critical element.

History of Electronic Voting Equipment

Hand-counted paper ballots began to be replaced by various mechanical devices early in the 20th Century. By the mid 20th Century, punch card technology was introduced in different implementations. In both of these innovations, counting was taken out of human hands and entrusted to mechanical or electronic machines. The tally reported by the machine at the end of the voting day was trusted to be the true count voted on that machine. Later, Westinghouse developed the optical scanning device. In this method of voting, the voter indicates their selection by filling in an area, and the cards are then read optically in high speed tabulation machines. Since the 1990s, a variety of direct record electronic (DRE) machines have been developed. At first, these were essentially electronic equivalents of mechanical level machines. Increasingly, however, they presented new form factors and technologies, such as touch screens and other innovations.

Election officials did not move to new technology without reason. Each new technology was adopted with the intention of solving important problems. A central issue has been that hand counting paper ballots is susceptible to human error and various kinds of election fraud. Elections rely on many people, mostly volunteers. Elections are relatively infrequent but long and demanding events. Poll workers and others involved in running an election work very long hours on Election Day, and are prone to make mistakes through fatigue or lack of practice. Further, paper ballots can be fraudulently removed from the process or forged ballots added in. Automation was added in an attempt to address these problems. However, the automation itself might be compromised. Today's challenge is to find the optimal mix of using automated systems but with safeguards to protect them. The question then becomes, what is the best combination of automation with manual checks to produce the most accurate, reliable and secure system achievable?

By analogy, it is entertaining to remember that, while today we are greatly concerned about air pollution from automobiles, our forefathers saw the automobile as a solution to a pollution problem. Horse pollution was a great problem in every street in the land. Returning to the horse and buggy will not eliminate pollution, but simply change the form of the pollution. Similarly elections had errors and were subverted with every system ever used. Every technological step introduced has claimed to improve the accuracy, reliability and security of the voting system. A review of history generally supports these claims as being accurate, with the understanding that no innovation has eliminated all problems. From a historical perspective, it may be argued that the original paper ballot system was the least secure, reliable and accurate system used in this country. The challenge today is how to get the most accurate, reliable and secure system possible.

The problems in the elections arena are multivariable and the solutions are compromises, attempting to simultaneously meet multiple, competing requirements. In the end, we want systems that are secure but user friendly. We want to have systems that allow the voter to verify their vote, but which also allow people with disabilities to vote in private. We want systems that protect the confidentiality of the vote but also allow effective audit and recount of the tally. We want the highest possible reliability and accuracy, while at the same time having systems affordable to all jurisdictions. The choices are among compromises and one size seldom fits the vast variety of voting jurisdictions.

Voting System Standards

The history of U.S. federal standards for voting equipment begins in 1990. It surprises many people that, prior to 1990, there were no federal standards for voting equipment. The first national standard was published in 1990 by the U.S. Federal Election Commission (FEC) Office of Elections Administration (OEA), which has now been incorporated into the U.S. Election Assistance Commission (EAC). Though voluntary in nature, the 1990 FEC standard introduced the first set of national requirements for voting equipment. It is of interest that the FEC produced this document without clear legislative authority to do so. Seventeen years later, it is easy to criticize the shortcomings of this document. However, at the time it was introduced, it filled a vital need, without legislative authority; simply through the power of doing the right thing, it began the process of setting minimum requirements for voting system.

However, a standard is not an end in itself but a tool. Standards become the specification documents for quality systems. The quality system is responsible for assuring that specifications are actually met. This need for a system to implement the standard was soon recognized and the National Association of State Election Directors (NASED) created a system of Independent Test Authorities (ITA) to provide a trusted source for evaluating equipment to the standard. NASED accredited and supervised a set of ITA laboratories. The ITAs provided a central evaluation of voting systems that states could use as a baseline pre-requisite for meeting state certification requirements. When the NASED certification program was transitioned to the EAC in 2006, approximately 40 states were participating in the program.

While laudable, the 1990 FEC standard was limited in many ways and, over time, became somewhat technically dated. The 1990 standard represented the first step in bringing consistency to what had previously been an industry that was independently regulated by each state. This standard went a long way but did not accomplish everything. In 1997, the FEC inaugurated a much needed revision of its 1990 document. The trauma of the 2000 election occurred before their work could be completed. Among the many lessons of the 2000 election was how prescient the FEC staff was in beginning that work. The revision was completed and adopted as the 2002 FEC standard.

After the 2000 election, through the Help America Vote Act, Congress created the Election Assistance Commission (EAC) and assigned it the responsibility of setting guidelines for voting systems and certifying voting systems as meeting those guidelines. The EAC, in collaboration with the National Institute of Standards and Technology (NIST), developed a new revision of the federal voting system standards. In 2005, the EAC issued its Voluntary Voting System Guidelines (VVSG).

Currently, the EAC with NIST, through a joint committee, the Technical Guidelines Development Committee (TGDC), is developing a new revision of the 2005 standards. This newest revision is expected to come out of Committee in the summer of 2007. It must then go through a very thorough and lengthy review process at the EAC before being adopted. One way of conceiving this process is that technical specialists bring their isolated recommendations on how to improve various components to the TGDC. Each specialist is anxious that the very best be done for this very important function, which is a foundation of our democracy. The TGDC organizes those recommendations into a draft specification. It is then the EAC's task to mature that recommendation into a standard that delivers its intended result all the way to the equipment used on Election Day, and which improves not isolated components but the security, accuracy and reliability of the entire system. Part of the EAC's challenge is to look at the resource allocation balance. When we spend more time on this, what are we spending less time on? It is not an easy assignment.

Certification Process

In 2006, the EAC officially inaugurated its voting system certification program, taking over the role previously filled by NASED. In July 2006, NASED announced that it would no longer accept systems for certification, and the EAC launched its program. The EAC program has many features in common with the NASED program but adds fundamental new functions. Under the EAC program, vendors must first register, submit their quality system, change management system and a great deal of additional material and qualify as a voting system manufacturer before they can submit a voting system for certification. The NASED ITA laboratories are replaced by NIST NVLAP (National Voluntary Laboratory Accreditation Program) recommended Voting System Testing Laboratories (VSTL). The EAC program adds field incident reporting and manufacturer facility auditing to the conformity assessment system. Taken together, the new features of the EAC program make it a major generational development from the NASED program.

However, like NASED, the EAC system is a voluntary program. Approximately 40 states have mandated that voting systems be certified by NASED in order to be certified at the state level. By this mechanism, the NASED voluntary program became mandatory in those states. A similar mechanism is at work with the EAC system. The EAC VVSG is a guideline and its certification program is entirely voluntary. However, most states require the use of the program, which then makes it mandatory for those states.

The system is made more complex by the fact that certification, both federal and state, is separate from the purchase decision. Typically, the final purchase decision is made by a city or county. The result is three levels of testing and evaluation before a system is purchased, followed by a receiving inspection before it is used in an election. At the federal level, the EAC is testing voting systems to the requirements of the VVSG. This testing might be characterized as assuring that a system meets the minimum requirements for a voting system used anywhere in the U.S. State certification is assuring that a system meets the minimum requirements for that specific state. It is during the procurement process that the best system for a specific jurisdiction is selected.

Figure 1 illustrates the multiple participants and diverse nature of the U.S. voting system certification process. This diversity can bring substantial benefit in that the system is reviewed independently by the EAC's VSTL and by multiple states. However, it also creates the possibility of oversights, primarily through misunderstanding and miscommunications.

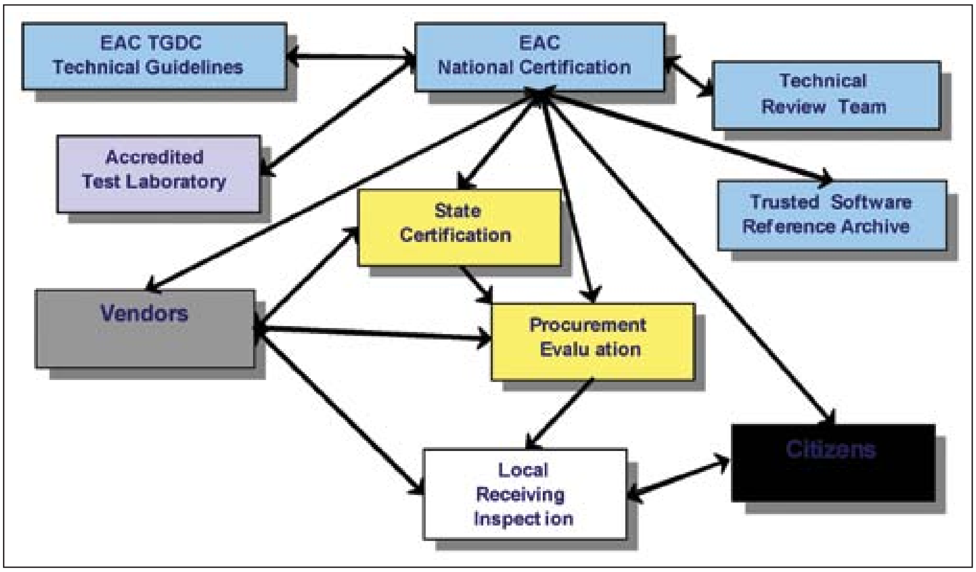

Figure 1: The diversity of roles and participates in the US elections conformity requires tools to assure effective coordination and communication.

Many people do not realize that no two states run elections in exactly the same way. Under the constitution, elections are a state function, and every state has its own set of procedures and rules governing elections. State certification focuses on whether a system meets the particular requirements of a state. This testing can be characterized as assuring that a system meets the minimum requirements of a voting system in a particular state. To be sure, there is overlap and shared concern between the federal and state certification.

However, in general, these sets of tests are evaluating different requirements. At their best, they are administered to coordinate efforts and be mutually dependent.

A particular jurisdiction will evaluate competing systems when making a purchase decision. The concern here is to determine which system is best suited and provides the best value for a specific jurisdiction. Notice that this is the only time the question of which system is best is being asked. Federal and state certification efforts determine if a system meets minimum requirements. Those minimum requirements are extremely rigorous but none-the-less they set a lower boundary on what is acceptable and unacceptable in a voting system.

There has been and continues to be a wide variation in state certification requirements. Voting systems are purchased by the designated election authority. This may be a city election commission, a county or the state itself. However, these systems must first be certified by the state before they may be sold, as has been the case for decades. Certification requirements varied drastically from state to state. Some states required a demonstration of the proposed equipment before the State Election Board, while others only required an application for certification. Still others required a full set of hardware qualification tests to be performed by a accredited laboratory.

In summary, the current U.S. certification system may be characterized as:

- Resource limited;
- Distributed (there are federal, state and local responsibilities);
- More periodic than routine;
- Having diverse and sometimes conflicting requirements;
- Required to balance real and hypothetical problems;
- Needing to prevent problems before they occur.

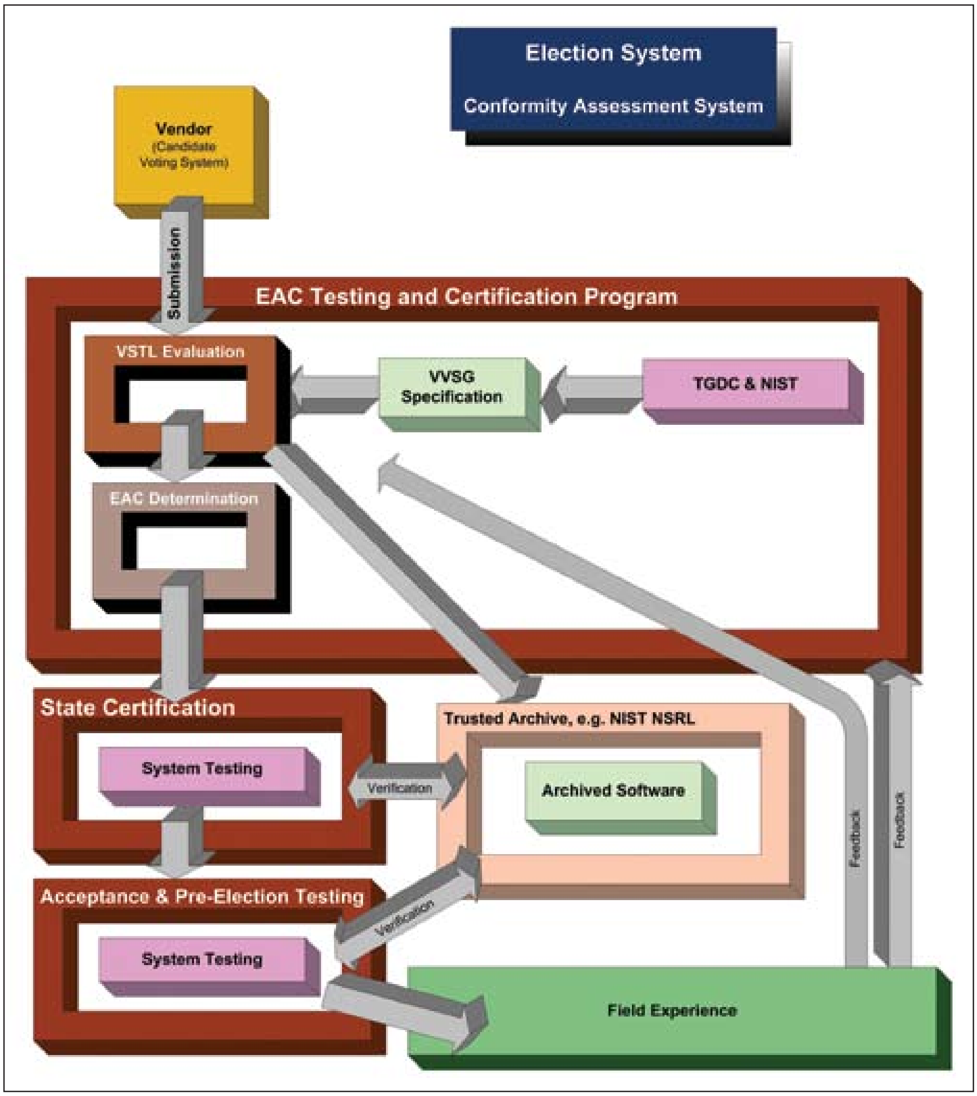

Figure 2: Voting Equipment Certification System

Trusted Software Archive

Those working in the field of elections conduct an ongoing effort to bring the best practices from other areas, facing similar challenges. The voting equipment industry is very small when compared to many other sectors. Approximately 40 companies participate in any way, and only about 6 companies have actually sold voting systems in the U.S. Therefore adopting solutions refined in industry sectors with far more resources brings to the election system a value that it could not develop itself.

In that vein, one such concept is the trusted archive or software repository, and the use of file signatures codes, often called HASH codes, to verify that software has not been modified. At the FEC-NASED meeting in Ft. Lauderdale, FL in 2003 NIST presented the function it provides to law enforcement for escrowing software. Through the use of various hash codes, it is possible to determine to an extremely high degree of certainty that the code being used in the field is the same code that is in escrow and which was examined and qualified.


Innovative Power Distribution
Solutions For Interference Protection
Harmonics
Noise
Frequency
Radiated Interference
Conducted Interference
RCP100-BLK-LT www.pulizzi.com/remote
TPC2365-LT www.pulizzi.com/international
- Emergency Power Off Control for test systems
- Safe - Low voltage dc control interface
- Control 120V, 208V or Three Phase Power Distribution Units
- Auto voltage selection for 120V, 208V or European 230V operation
- EMI/RFI filtering of input power - CE mark
- Remote interface for connection to ON/OFF/EPO panel
Z-LINE
PULIZZI®
ENGINEERING, INC.
1-877-PULIZZI
(785-4994)
for more information and online ordering visit: www.pulizzi.com
Made In The USA
CFM0207

Because certification and procurement of voting systems is distributed and done by different parties in different places, it is particularly important to have safeguards to ensure that the exact same system and system software are being reviewed. The federal, state and local evaluations add value to each other. However, this value only exists if they are all looking at exactly the same system. It is not widely known that some states do not allow vendors to deliver software directly. Rather, under the NASED system, the ITAs supervise a compilation of the code they examine, and then the ITA delivers the code to those states, after it is approved. Texas and Georgia are two examples where it is the ITA, not the vendor, that delivers software to the state. This safeguard provides a double witness to the process. The test lab attests to the state that the software they are sending is what they certified. During the exam, the vendor ratifies that the software being evaluated is what they submitted for certification. Further, it assures that the national and state examinations are viewing the same code and therefore building on each other. Another little known fact is that in some states, like Florida, a vendor must escrow with the state a sample of the software for each particular precinct tabulator. This escrowing of software and control of it through the examination process not only increases the confidence in the original examination, but assures that, should questions arise at a later time, further examination may be made of the same code.

Using file signature codes with this system adds further security. By running various file signatures codes on the software an examiner reviews, and then running the same codes on the software loaded onto individual systems in the field, it can be proven with high degree of reliability that the code being used in the field is the same code that was examined. These codes can then be compared to the values from a trusted archive, listed on a web site, to confirm that the software has not been modified in any way.

Even better, as the code is reviewed again at the state level, it can be assured that the code that was reviewed at the national level is the same code being looked at by the state examiner. More states are performing their own source code review and performing operational tests of voting system software. As examiners in different states can be sure they are looking at the same code, their examinations build on each other's efforts. As the software goes through multiple reviews, confidence in it rises.

However, all of this assumes that there is enough consistency and redundancy and that there are overlapping checks at the national, state and even local level. Fragmentation of requirements and election practices is a major obstacle to capturing this benefit. Encouraging consistency in the core functions of elections is important if the election system on a national level is to be improved.

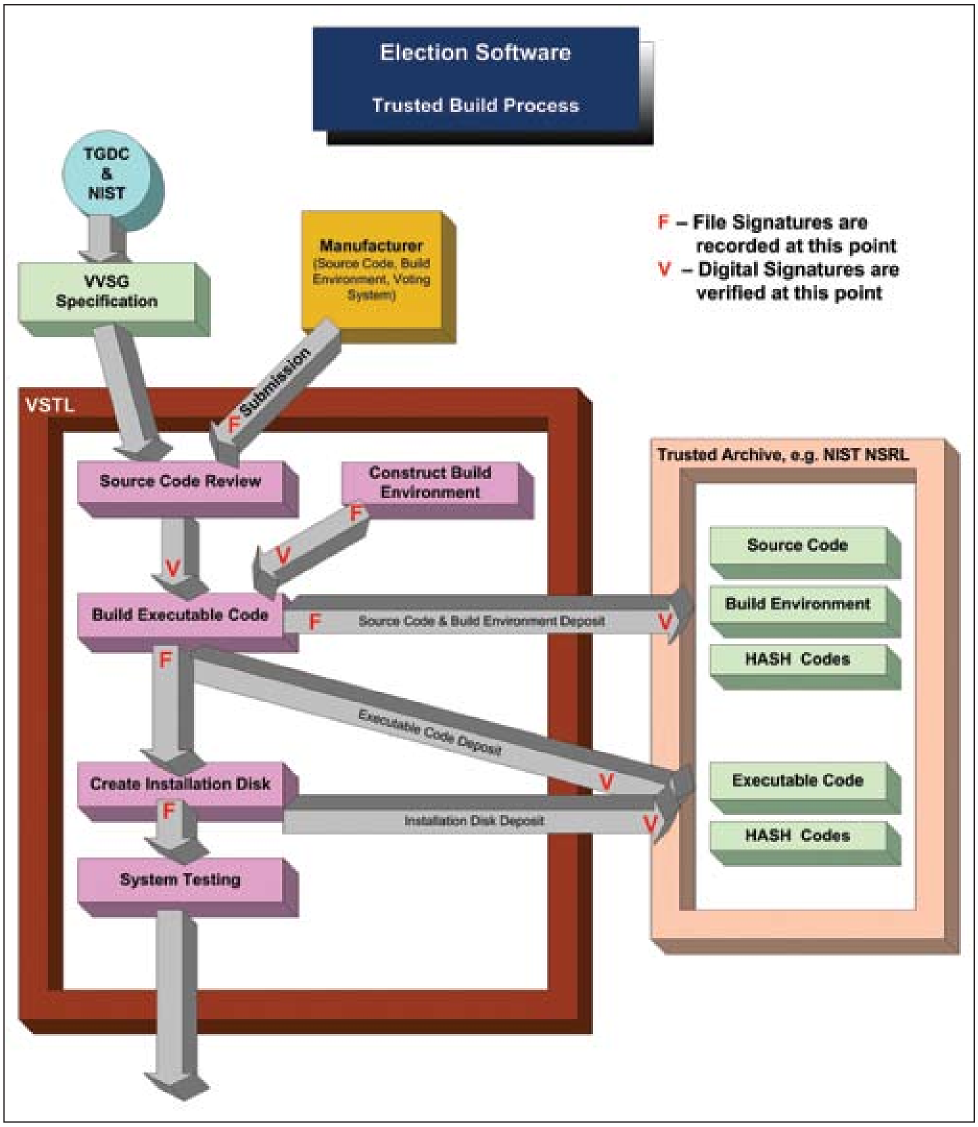

Figure 3: The Trusted Build

Trusted Build

A component of the NASED certification process was the witness build[1]. The vendor initially delivered their source code to the ITA for source code review. After the software was successfully reviewed and approved, a witness build was performed. Representatives of the

ITA and vendor together built the source code into executable code. The ITA personnel then installed the resulting executable code and used that code for the remainder of the testing of the voting system.

The EAC in its certification system has extended the concept of a witness build and called the new procedure a trusted build. The process is similar to the NASED process, with the addition of file signature generation, multiple points of verification, and the archiving of the software source and executable code. There are other safeguards introduced by the EAC to give greater assurance that the executable code produced from a build is a faithful implementation of the source code that was reviewed. One of these additional features is a requirement that the build environment be constructed with the VSTL personal supervising. Further file signatures are taken not only of the source and executable code but of the build environment. These measures not only protect the integrity of the process, but produce forensic records that can be used should future investigations become necessary.

EAC's Conformity Assessment Systems

Like most regulatory agencies, the EAC constructed its program using guidelines from ISO 1701. Because of the critical importance of safe and secure elections, the system is extensive, incorporating features like vendor site audits and field surveillance, which are usually adopted in programs only when the consequences of failure are very severe. It was well recognized by the EAC that one of the distinguishing characteristics of elections is that, if there is a failure, the remedies that can be applied after the fact are few and onerous. Therefore, it is of utmost importance that problems be prevented. The EAC has incorporated the following elements into its program:

- Type testing/design evaluation;
- Assessment of the supplier's quality and change management system;
- Field surveillance;
- Field management/enforcement;
- Training of personnel and ongoing communication with stakeholders;
- User outreach.

To understand the far reaching change that has been implemented takes only a brief consideration of the history of voting equipment certification. Before 1990 there were no national requirements for voting equipment. Certification was controlled by the states and the rigor of the certification evaluation was highly variable. In 1990, a standard was adopted by the EAC but there was no system to implement it. NASED established the first national certification system in 1994. That system could be generally characterized as limited to testing a representative sample system and certifying the design as meeting the requirements of the 1990 standard. Because the system was conducted by NASED, there was a significant but largely informal system of field surveillance. State election directors knew how the systems performed in their states and those insights were fed back into the process. However, it is fair to characterize the new EAC certification process as the first full conformity assessment system to be implemented in the U.S. As of early 2007, no voting system has been certified by the EAC and so the benefits of the new system won't be realized for some time.

Current Challenges

Despite the far reaching reforms that have been initiated, efforts intended to bring further improvement are being vigorously pursued by many parties. There are several areas currently receiving particular scrutiny for further improvement. However, in each case there is a real need to develop a short term and long term solution with a transition plan between them. This is very difficult to accomplish but absolutely necessary. Figure 4 lists some of the areas currently being reviewed and illustrates this concept of transitioning from short term to long term solutions with a planned phase over.

As Table 1 illustrates it takes 4-8 years to implement a change to the national requirements. While that is a long time, for a process of this importance, nobody wants to see changes made without careful review. Each step of the process takes time and many are mandated by legal requirements. As examples, the EAC must follow U.S. government rule-making requirements and states and local jurisdictions have firm procedures governing their contracting processes. Both the EAC and state election officials understand and value public comment, but that takes time to receive and process. The cumulative result is that, when a change is desired, it is necessary to ask how much can be accomplished with the equipment and processes that currently exist, while also planning for a more desirable implementation for the long term.

The first issue listed in Figure 4 is the coordination of EAC and state certification efforts. The EAC program is new and has yet to certify a voting system. At this time, state certification efforts operate independently of the EAC's effort and from each other, except that most require the completion of national certification before state certification can begin. There are opportunities that are being missed. One example arises when state certification review identifies improvements desired by a state. At that point, the vendor has their national certification and cannot modify the system without submitting the modifications to the EAC. Further, different states typically identify different desired improvements. A more coordinated system might find some means to allow the vendor to implement these requested improvements and resubmit in some facilitated certification process. There are challenges to be sure; however, facilitating the introduction of good improvements while protecting the integrity of the certification system is a fertile area for further improvement.

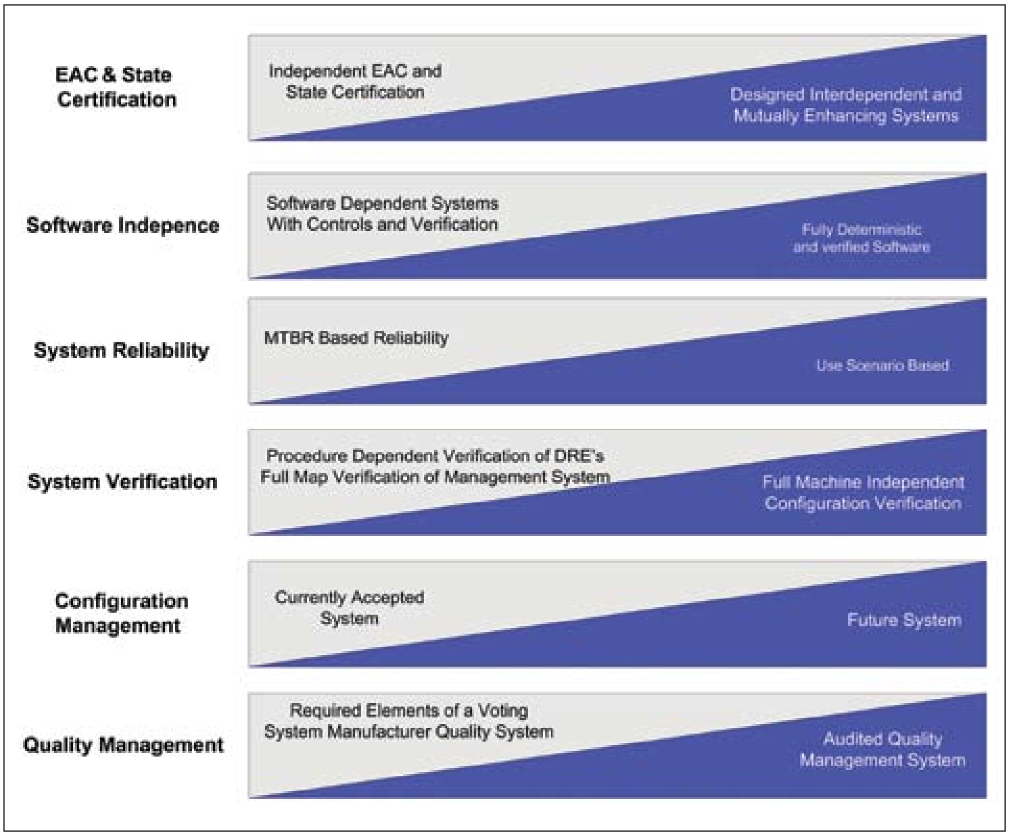

Figure 4: Transition challenge for areas currently being considered for improvement

The popular voter verified paper ballot has lost some of its luster now that many states are actually using systems that print a receipt of the voter's ballot. There are few enthusiasts for the verified paper ballot process as currently implemented. Given the popular appeal of the voter verified paper ballot, a lot of effort will almost certainly be invested in addressing the deficiencies of the first crop of machines to implement this method.

Protecting voting systems from the possibility of software errors is a high priority. In the short term, a lot can be done to assure that voting systems only use certified, source code reviewed and thoroughly tested software, and that this can be independently verified. In the long term, creating systems with fully deterministic software that can be proven to be error free would seem to be the goal.

System reliability is another area under study. Currently systems are tested to a Mean Time Between Failure (MTBF) requirement. However, in elections the important thing is not how long the equipment lasts, but whether thousands of units be stored for long periods of time, brought out of storage, and used with high degree of reliability. Voting system reliability needs to be evaluated based on its use scenario rather that MTBF approach.

Other areas currently being discussed are the ability to verify that systems, software and hardware are unmodified from their certified condition, configuration and quality management. Each of these areas offers opportunity to improve what is currently in place and the promise of more thorough improvements in a longer timeframe.

Future Developments

Some of the most promising efforts in the field of elections are the development of electronic data interchange standards, introduction of public/private key infrastructure (PKI) security and standardized voter registration databases. A more distant future possibility is the introduction of a model driven architecture for voting systems. A particularly encouraging phenomenon is the emergence of university-based elections technology centers, which go a long way to speed these efforts forward.

Electronic Data Standards

Electronic Data Interchange (EDI) standards define the inter-organizational, computer-to-computer exchange of structured information in a uniform and machine-processable format.[2] EDI standards establish a common format to allow the transmission of information from one computer application to another by electronic means and with a minimum of human intervention. Typically, EDI is understood to mean specific interchange methods agreed upon by national or international standards bodies for the transfer of business transaction data. Some of the more common applications are the automated purchase of goods and services, money transfers or exchange of common business documents such as purchase orders and invoices.

EDI standards serve as tools supporting larger processes. When used in a model driven architecture, they define what information must be transmitted at various points in the system and provide a common format for that information. EDI standards assist equipment certification by allowing common, vendor independent tests to be developed. They support other components of a larger conformity assessment system, assisting in the development of common audit practices and parallel testing. EDI standards also are necessary for a modular architecture, although they are not necessarily sufficient for that purpose. To assure the components from multiple vendors will work together, EDI standards must have sufficient detail and definition to rise to the level of interoperability standards.

Change Implementation Process	
Task	**Timeframe (months)**
TGDC proposal through EAC review and rulemaking to approved revision to VVSG	6 - 12
Grandfathering and transition period to new version of the VVSG	24
Vendor submission through VSTL testing to EAC certification	6 - 12
EAC certification to state certification	6 – 12
Contract solicitation for proposal to award of contract	3 – 6
Vendor receipt of contract to delivery of equipment	3 – 9
Training on new equipment and deployment for use	3 - 6
TOTAL (months)	**51 - 81**

Table 1: Change implementation timeframe

Because EDI standards are tools enabling higher purposes, it is important to understand those purposes. EDI standards are most effectively developed with a specific use(s) in view, if they are to be written to optimally serve their intended function. Data standards and, as presented in the next section, a model driven architecture have the potential for bringing improvements in several of these areas. Having common data standards would allow more automated and uniform testing, thereby making better use of scarce resources. Development of uniform test methods allows the pooling of resources through more effective sharing of test tools, methods and data. The periodic nature of elections relies a great deal on the institutional memory of the participants. Data standards and system models become tools, supporting systematic review of systems for certification or pre and post elections checks. They become analogous to a pre-flight checklist for aircraft, ensuring that all items are correct. Having common data standards supports the introduction of new audit tools. For example, third party equipment could be introduced at selected points in the system to audit the vendor's equipment and provide an independent verification its operation.

Model Driven Architecture

A model driven architecture is a way of describing a system using a platform-independent and vendor-independent model. The Object Management Group[3] has refined and structured the process by developing a Unified Modeling Language (UML) to support formal Model Driven Architectures (MDA). A complete MDA specification has three levels, a Computer Independent Model (CIM), a Platform-Independent Model (PIM) and a Platform-Specific Model (PSM). UML is a tool that allows a tight connection between the CIM, PIM and PSM models, ensuring that each is an accurate implementation of the other. So an MDA set consists of a computer and platform-independent base UML model, with one or more platform-specific models and interface definition sets. Each set describes how the base model is implemented on different platforms, potentially by different vendors. A new derivative standard from UML, SysML has been developed to better model entire systems.

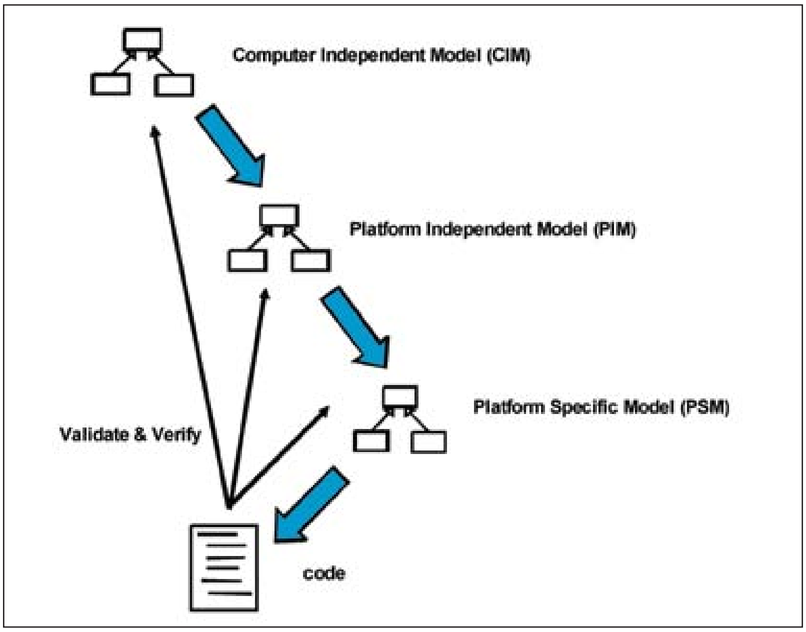

Figure 5: Key concepts of Model Driven Architecture (MDA)[4]

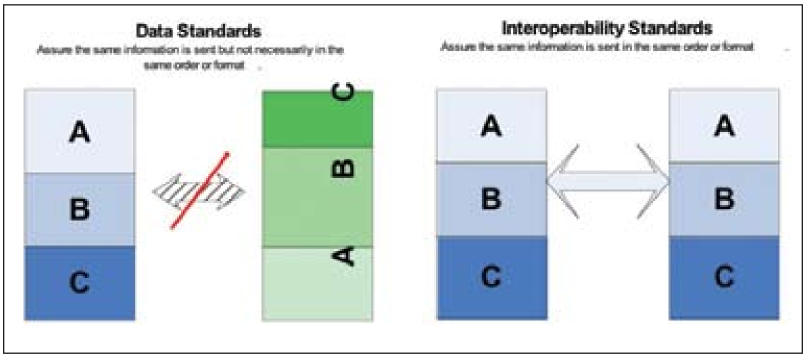

Figure 6: Data standards assure that the same information is transmitted. Interoperability standards assure that equipment will work together.

The MDA focuses primarily on the functionality and behavior of a distributed application or system, not the technology in which it will be implemented. It separates implementation details from functions. This allows all systems to be analyzed, and for high-level, universal requirements to be developed. The lower level models bring forth implementation nuances and require decisions on how high-level requirements will be realized using specific platforms and architectures. With MDA, functionality and behavior are modeled only once. OMG has invested a great deal of effort developing tools to assure that new or different technologies properly implement the high-level model.

Data Standards and Interoperability

Data standards and interoperability standards are two related but different concepts. Interoperability standards must go further than data standards to assure that all compliant equipment can interoperate.

EDI Standards for Voting Systems

There are currently two EDI standards being developed for voting systems. One project is being conducted by OASIS (Organization for the Advancement of Structured Information Standards)[5] and the other by the IEEE (Institute of Electrical and Electronic Engineers)[6]. The OASIS project is heavily dependent on the support of the United Kingdom's (UK's) e-Envoy office, which provides its chair. Accordingly, the OASIS project is flavored by European election processes and particularly the directions being explored by the UK for e-voting.

The IEEE project is primarily vendor driven. Its chair works for the largest manufacturer of voting systems, Election Systems and Software, and major contributions have come from other vendors, notably Hart Intercivic's contribution of the EDX schema. However, some people participate on both projects and each seeks to address its limits and deliver the best possible standard.

OASIS

OASIS was the first organization to begin work on EDI standards for voting systems. OASIS mission is to drive the development, convergence and adoption of e-business standards. This mission was extended to elections with the formation of its OASIS Election and Voter Services Technical Committee in March 2001. The committee, chaired by John Borras, Director Technology Policy for the UK Office of the e-Envoy Cabinet Office, has produced a standard for an Election Markup Language (EML), currently in its fourth version. EML was used in the local elections in Flanders on October 8, 2006. The UK's Secretary of State for Constitutional Affairs and Lord Chancellor, Lord Falconer of Thoroton, announced in January 2007 that 13 local authorities have been accepted to hold electoral pilots at the May 2007 local elections using EML. The committee plans to submit its next version for adoption as an ISO[7] standard.

IEEE P1622

IEEE initiated its own project, P1622 "Standard for Voting Equipment Electronic Data Interchange" in June of 2002. The committee, chaired by Peter Zelechoski of Election Systems and Software, is anticipating submitting their draft standard for approval ballot by mid-2007. In its current draft, P1622 defines the structure and elements of electronic exchange of voting system data and gives two reference implementations, EDX[8] and EML[9]. While there are important differences in these standards and specifically the EDX and EML implementations, the commonality of structure and elements dominates.

Correspondence of OASIS to P1622 Data Records

Although the OASIS EML defines 28 in contrast to the 7 IEEE P1622 data exchange records, there is substantial correspondence. The differences are driven by the somewhat differing purposes of the two efforts. OASIS is looking at the entire election process, supporting a European environment where Internet voting is being actively explored. The IEEE 1622 has a more restricted focus of data exchanges within a voting system, and reflects U.S. election processes more strongly. As the P1622 document identifies, it is possible to use the OASIS EML to implement the P1622 data records.

A survey of the data records not included in the IEEE document reveal the differing purposes in the projects. The OASIS project envisions the possibility of Internet voting, defining records that are exchanged during the voting session. These voting session records are contained within the voting station for in-person voting and so do not need definition where the voting will take place in a single session with the voter present. Other records, such as candidate nomination, are part of the larger election process and not part of most voting systems. Understanding these differences helps to understand the commonality and differences between the two standards.

Benefits of Common Data Standards

There are a number of benefits that can be envisioned from implementing common data standards and a model driven architecture for voting systems. Among the benefits most commonly named are:

- Independence from a single system vendor;
- System upgrading;
- Improved testing and certification;
- Improved security and election auditing.

Public Key Infrastructure (PKI)

The use of PKI (Public Key Infrastructure) technology to digitally sign data records is a powerful technology that is widely used, providing extensive benefits to many fields. There are many ways that this technology could be used in voting systems. One possibility is for the EAC to digitally sign all software after certification. Voting equipment can be design to refuse to load any software without proper authentication. This technique is used in many places today, including on iPods. A second security wrapper could be added and signed in each voting station. This would allow tabulation software to record the number of votes it received from each voting station and validate that the vote was produced using certified software. Automated audits would then be possible to assure that all voting stations had reported, and that no votes were included other than those coming from authorized voting stations.

PKI technology is mature and proven. It is widely and effectively used for a variety of purposes. The primary risk to

	OASIS EML Data Records	IEEE P1622 Correspondence
1	Election Event	Election Definition (partial)
2	Inter Database	
3	Response	
4	Candidate Nomination	
5	Response to Nomination	
6	Candidate List	Election Definition (partial)
7	Voter Registration	
8	Election List	Voter Roll
9	Polling Information	
10	Outgoing Generic Communication	
11	Incoming Generic Communication	
12	Internal Generic	
13	Outgoing Channel Options	
14	Incoming Channel Options	
15	Ballots	Ballot Form Election Definition (partial)
16	Authentication	
17	Authentication Response	
18	Cast Vote	
19	Retrieve Vote	
20	Vote Confirmation	
21	Votes	Cast Ballot
22	VToken Log	Voting History
23	Audit Log	
24	Count	Tabulation Report
25	Result	Post Election Canvas Result
26	Options Nomination	
27	Options Nomination Response	
28	Options List	

Table 2

its introduction in elections is from a flawed implementation that does not properly make use of the current state-of-the-art. The risk of flawed implementation exists for all promising innovations and is a very real risk in a resource constrained environment. Among the significant improvements the introduction of PKI technology offers are:

- Assure that only certified software is used;
- Require voting equipment to reject any improperly signed software;
- Link cast votes to voting stations;
- Allow election management to identify all voting stations reporting and exclude any votes coming from unauthorized voting stations;
- Allow automated checks for multiple entry of votes or machines not reporting in to the tabulation software.

Elections Technology Centers

A new and very encouraging development is the emergence of permanent elections technology centers. Universities have a long history of contributing their thoughts on the elections process. After the problems of the 2000 election, Cal Tech and MIT formed a joint project to study voting systems and the elections process. Researchers at Stanford, Johns Hopkins, Princeton and Rice have been widely quoted in the press on various aspects of voting systems and election processes. However, these efforts have largely been hit-and-run engagements, unencumbered from a significant engagement with election administrators. The various conclusions advanced generally do not wrestle with whether the innovations proposed increase or decrease the total system security and reliability. It is generally left to election administrators to wrestle with the competing risks of accumulated and compounding human error versus failure of a voting system. Regretfully, how to achieve an optimized system solution has been largely ignored by the academic community.

A striking contrast to this trend is found in the Election Center at Kennesaw State University. The Secretary of State of Georgia has funded a permanent center to support election officials. The Election Center provides technical support for election officials throughout the state, performing functions like equipment evaluation, verification of systems before deployment for use, ballot layout and software archiving. The Center also has been a useful resource for taking on special projects and developing tools needed by election officials. One such tool is a self-booting CD that automatically checks the file signatures used in election management systems. This CD, developed by computer forensics experts, makes a rigorous check that all software involved in election management remains unmodified, election to election.

More recently, a consortium of universities in San Antonio, lead by the Center for Cyber Security Policy at Our Lady of the Lake University (OLLU), has entered the arena. OLLU's consortium strives to replicate functions at the Kennesaw State center, and also adds a legal analysis and public policy component through cooperation with the School of Law at St. Mary's University. The OLLU effort seeks to unite a coalition of university centers of excellence to form an ongoing election support capability. The notable element in the Kennesaw State and OLLU efforts is their close collaboration with election officials. This arrangement mandates that these efforts deal with total system accuracy, reliability and security. The appealing escape of simply ignoring the most difficult problem of how to improve a system that, for a federal election, involves almost a million people (mostly volunteer) working long hours at largely unfamiliar tasks, cannot be avoided.

What to Change?

A particularly difficult challenge at this time is what further changes should be made to improve the certification process and election administration. Currently systems are being certified to the 2002 FEC standard. While the 2005 EAC standard has been out for almost two years, no system has yet been certified by the EAC to it. The TGDC is working hard on the next revision to the 2005 standard. One wonders how they know what needs improvement without seeing how effective the 2005 standard is.

A further complication is that, while the EAC program has been inaugurated, many of its features have yet to be implemented. Here again, making further changes while these reforms are being implemented brings real questions as to the total end result when everything is finally realized.

Unintended consequences are a real, ongoing and too frequently experienced danger. It is the author's estimate that the cost of testing has doubled or even tripled with the 2002 standard, in contrast to the 1990 standard. Early estimates of the cost of evaluating equipment to the 2005 standard look like that transition will double or triple costs to the 2002 standard. In response, vendors are grouping changes and bringing systems in less frequently for certification. This further complicates the certification process. Further, it delays needed improvements because it is simply too expensive to certify system modifications one at a time. However, who could credibly recommend that certification of voting equipment be less demanding?

Today, we find a field with many changes being implemented, new initiatives proposing yet further changes, and the very real potential that the cumulative total result may bring some very unwelcome consequences.

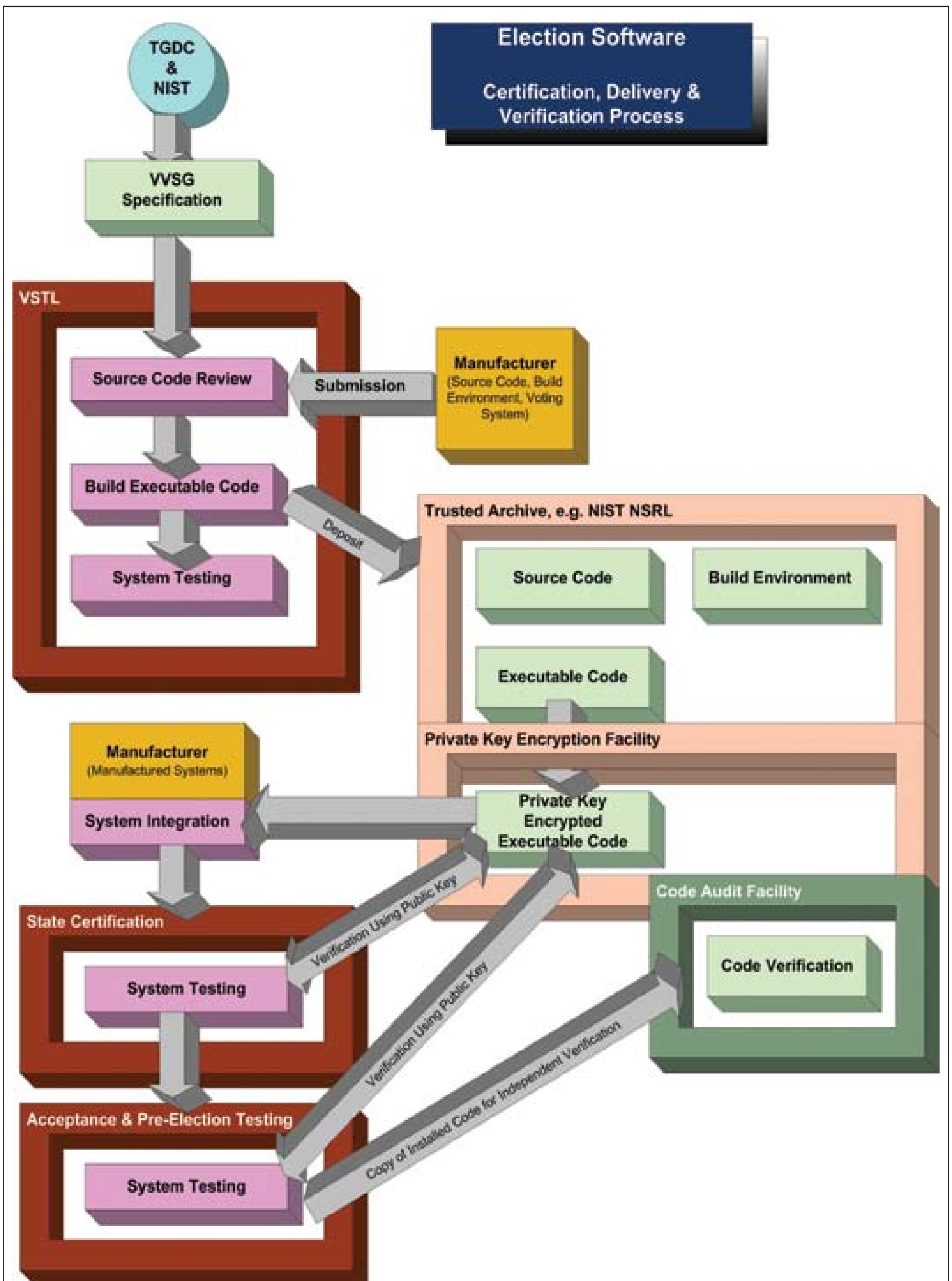

Figure 7: Integration of PKI to delivery and verification process

Conclusions

Voting systems and elections are far more complex than generally perceived. The certification of voting equipment is a diverse and rapidly changing process. It is encouraging to see the many contributions being made and new innovations being introduced. However, the concern over unintended consequences and conflicting requirements makes the field extraordinarily demanding. Given its complexity and built-in ambiguities, the high level of accuracy and security delivered by election officials is a real testament to their dedication and extraordinary efforts.

New technologies and system tools have great promise for improving the system. It is particularly encouraging to see the rise of permanent university-based election centers that operate in close partnership with election officials to deal with system issues and consider the total system impact of innovations. □

Stephen Berger *is the principle of TEM Consulting, and can be reached at stephen.berger@ieee.org.*

Notes

1. A build is the process of converting source code into executable code. Source code is software in a form readable by a programmer. Executable code is software converted to a numeric form, which is the only thing computers understand.

2. www.orafaq.com/glossary/faqglose.htm

3. www.omg.org

4. Figure adopted from a presentation, "OMG's MDA and Software Radio," presented January 25, 2006 at the IEEE 1900 plenary meeting in Boulder, CO by Fred Waskiewicz, Director of Standards Object Management Group, wask@omg.org

5. OASIS describes itself as "a not-for-profit, international consortium that drives the development, convergence, and adoption of e-business standards. The consortium produces more Web services standards than any other organization along with standards for security, e-business, and standardization efforts in the public sector and for application-specific markets. Founded in 1993, OASIS has more than 5,000 participants representing over 600 organizations and individual members in 100 countries." For more information on OASIS see www.oasis-open.org/specs/index.php.

6. http://standards.ieee.org

7. ISO, the International Organization for Standardization, is a leading developer of international standards. For more information see www.iso.org.

8. EDX (Election Data eXchange) is an XML (Extensible Markup Language) schema submitted by Hart InterCivic.

9. EML (Election Markup Language) is an XML schema provided by the Organization for the Advancement of Structured Information Standards (OASIS).

FAST Link www.conformity.com/0550