Certification of ICTs in Elections

Certification of ICTs in Elections

Certification of ICTs in Elections

Contributors:
Jordi Barrat
Eden Bolo
Alejandro Bravo
Robert Krimmer
Stephan Neumann
Al A. Parreño
Carsten Schürmann
Melanie Volkamer
Peter Wolf

International IDEA Resources on Electoral Processes

International IDEA
Strömsborg
SE-103 34 Stockholm
Sweden
Tel: +46 8 698 37 00, fax: +46 8 20 24 22
Email: info@idea.int, website: www.idea.int

International IDEA encourages dissemination of its work and will promptly respond to requests for permission to reproduce or translate its publications.

Cover design by: KSB Design
Graphic design by: Turbo Design, Ramallah
Printed by: Bulls Graphics, Sweden
ISBN: 978-91-7671-028-9

Preface

Information and communication technologies play a critical role in the administration and organization of modern elections. Any breakdown of an election technology, security breach or programming error can incur tremendous cost for the electoral management body (EMB)—and may undermine voters' trust, reduce voter participation or even cause national unrest. Not all of these problems are avoidable, but in most cases, good quality control can significantly reduce the likelihood that they will occur.

This publication is a guide on how best to achieve quality control in election technologies, such as electronic voting or tabulation systems. The key elements of quality control are *certification* and *evaluation*. Certification refers to the confirmation of proof of compliance with a given standard. Evaluation is the most labour intensive part of the quality control process, during which the requirements, designs, hardware, firmware, software, networks and operational contexts are examined for faults. Elections technology can only be certified by third-party reviewers who are accredited to assess compliance with a standard.

An EMB should consider quality control early in the process of introducing new technologies, starting during the feasibility study, especially if it is bound by law to provide such a certification. The evaluation reports and related documents can also be used to increase transparency of the election, improve the dialogue between EMBs and voters, and increase the EMB's credibility.

Yves Leterme
Secretary-General
International IDEA

Acknowledgements

We would like to thank all those who contributed to the content of this Guide, in particular the authors who patiently sat through an intensive five-day drafting workshop in order to generate its content. We thank Jordi Barrat, Professor of Public Law, University of Catalonia/URV, Spain; Eden Bolo, Technical Evaluation Committee, Commission on Elections, Philippines; Alejandro Bravo, Specialist of the Department of Electoral Cooperation and Observation at the Organization of American States; Robert Krimmer, Professor of e-Governance, Tallinn University of Technology, Estonia; Stephan Neumann, Research Associate and Doctoral Student, Technical University Darmstadt, Germany; Al A. Parreño, Electoral Commissioner, Philippines; Carsten Schürmann, Associate Professor/DemTech, IT University of Copenhagen, Denmark; Melanie Volkamer, Assistant Professor at the Technical University of Darmstadt, Germany; and Peter Wolf, Technical Manager, Electoral Processes, International IDEA.

Last but not least, we would like to thank Faith Bosworth, facilitator of the Book Sprint workshop, for keeping the contributors on track; Raewyn Whyte for proofreading at night time and Kelley Friel, for her meticulous language editing of the Guide; and International IDEA colleagues, Tendai Chinamora-Jönsson, for her logistical support, and Publications Officer Lisa Hagman for seeing the Guide through the editing and production stages.

Acronyms and abbreviations

AES	automated election system (Philippines)
BIOS	basic input/output system
CoE	Council of Europe
COMELEC	Commission on Elections (Philippines)
E2E	end-to-end verification
EAC	Election Assistance Commission (United States)
ECI	Election Commission of India
EMB	electoral management body
EVM	electronic voting machine
ICE	international certification entity
ICT	information and communications technology
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
IT	information technology
NDA	non-disclosure agreement
NSWEC	New South Wales Election Commission (Australia)
OAB	Ordem dos Advogados do Brasil (Brazilian Bar Association)
RFI	request for information
ROM	read-only memory
TEC	Technical Evaluation Committee (Philippines)
TSE	Tribunal Superior Electoral (Brazil)
VEC	Victorian Electoral Commission (Australia)
VSTL	Voting System Test Laboratory (United States)
VVPAT	voter-verified paper audit trail
VVSG	Voluntary Voting System Guidelines (United States)

Contents

CHAPTER 1

Introduction

About this guide

Technology is used in elections to achieve two objectives: (1) to ensure that all information produced during the electoral process, particularly the election results and the electoral roll, is correct and trustworthy and (2) to generate broad acceptance that the electoral outcome is a true and fair representation of the citizens' will.

The use of technology in elections is growing. Computers increasingly perform many tasks that were previously undertaken by humans. Election technologies are not standard, off-the-shelf software systems; they are usually complex solutions customized to the specific needs of each electoral management body (EMB). Since elections represent a country's individual constitutional and democratic culture, they have their own distinct regulatory frameworks, focuses and voting procedures. Thus election technologies are (and will always be) context specific.

When introducing or operating critical information and communications technologies (ICTs) in elections, EMBs must usually assure themselves and other stakeholders that a given technical solution fulfils national legislated requirements, is secure and trustworthy, is of high quality, and will avoid failures and perform as expected.

Certification of technologies, such as electronic voting or tabulation systems is often seen as an option for providing this assurance. Certification practice varies greatly between countries and EMBs; some do not do any, while others use very distinct processes with vast differences in scope. The process is made more complex by the fact that the related terminology is not well defined. Expectations as to what certification can achieve, and assumptions about the

resources required for certification, are often not realistic. Most importantly, certification can **not**, on its own, create democracy or trust in the process.

- Certification will not automatically confirm that the electoral process is 'in line with international standards for elections' or conducted 'according to best practice'. The integrity of elections and the resulting democracy depends on much more than technically certifying equipment and processes.
- It is not a means of importing democracy, and it should not be used as an argument to reject criticism of the electoral process or the technology used.
- It is not a quick solution to establish trust in the chosen election technology. Certification is a complex process that usually involves devoting considerable time and resources in addition to satisfying detailed technical requirements. While some of these requirements can be derived from legal frameworks or international obligations and standards, there are currently no comprehensive, globally agreed technical specifications for election technology.

However, certification **can** assure national and international stakeholders that an election technology has been thoroughly and independently examined. It can also ensure compliance with a quality management system to maintain certification, including the implementation of continuous monitoring and improvement plans. The detailed scrutiny that is part of the certification process can lead to the discovery of shortcomings that may otherwise have remained undetected. A clear understanding of the requirements for certification, and a public announcement that these requirements have been met, can increase public confidence in the election outcomes.

Since using a certified system reduces the risk of technology failure on election day, the certification process provides additional assurance that systems will work as planned. Moreover, certification can give vendors clear requirements for developing systems. If such requirements are formulated at a national or even international level, it is easier for vendors to provide exactly the systems needed. If vendors can get their products certified on the basis of meeting these requirements, it becomes easier to market these products in the jurisdictions for which the certification is valid.

This Guide aims to help stakeholders better understand the significance of certifying election technologies, what certification can and cannot deliver, and how it can be conducted and communicated.

How to use this guide

This guide is designed to assist EMBs in designing a sustainable quality control process and planning for the process of reaching certified compliance with a given standard. It also aims to help EMBs and other interested stakeholders such as non-governmental organizations assess how to use the outputs of this process (such as evaluation reports) to create transparency in the electoral process.

Chapter 2 provides an overview of what certification means and what it provides, and helps to dispel common myths about certification. Chapter 3 introduces the electoral cycle and identifies technologies and processes that could be targeted for certification. Chapter 4 describes the Quality Assurance Framework in detail, which was written to help guide EMBs and other stakeholders through the necessary steps of certification and evaluation tasks.

Chapter 5 outlines the relationship between legal and technical requirements—understanding these is necessary for a successful certification. Chapter 6 describes a host of issues regarding the allocation of resources, and discusses ways to use the different outputs of the certification process to make the electoral process more transparent.

Finally, the case studies in Annex A summarize efforts to certify and evaluate election technologies in a number of countries, while Annex B contains an overview of relevant standards and describes an approach to help precisely express and communicate the separation of duties.

CHAPTER 2

Why Certify (or Not)?

Criticism or excuses?

The utility of certification processes is often questioned during the implementation of election technologies. The following are examples of such criticism.

Certification is only a lot of bureaucracy without added value. Certification contributes to the democratic nature of elections and is therefore worth the effort. Introducing a full-fledged certification process not only increases the transparency of the election technologies under evaluation, it also contributes to the division of power and by that to the democratic nature of the election. Ideally, a certification process will give (almost) all electoral stakeholders a higher level of confidence that the election technologies will:

a) live up to their expectations;
b) be free of obvious mistakes;
c) be documented such that experts and future users can understand and operate the technologies properly; and
d) provide an effective means of control to all electoral stakeholders—not just the immediate users within the EMB.

Certification lacks the flexibility needed for an agile IT project. IT projects are complex to implement, which makes them prone to delays. Certification requires even more time after project completion, and once a system is certified there is limited scope for any last-minute changes. However, bottlenecks can be overcome by using proper procedures and a legal framework that allows necessary updates and changes to the configuration of certified systems. Systems developed and completed too late are still unlikely to be certified, which is also an indication of the higher risk and lower quality of such last-minute developments.

Certification is too expensive. Although a fully-fledged certification process can be costly, it is much less expensive than a failed election. Spending money on a process that increases transparency and facilitates a better division of power is a wise investment. Considering resource limitations, it may still be necessary to prioritize critical components for certification.

There is no such thing as an independent third party. Any third-party certification body needs to be contracted and paid by the EMB or the system vendor, which calls its independence into question. Beyond such financial concerns, stakeholder perception will determine which third parties are deemed independent enough. For example, international certification bodies are considered undue foreign influence in some contexts. Conversely, in a politicized context, many qualified domestic institutions may be deemed biased; some countries will regard academic institutions and other commercial certification bodies as more acceptable. Regardless, it is important that the selected body enjoys widespread acceptance among all stakeholders.

Certification takes up too much time in our tight schedule. When implementing election technologies, missing a deadline often results in either using an unfinished product or postponing its use until the next election. Without careful planning and dedicating enough time to project implementation, successful usage of election technologies is hard to achieve. This general principle also holds true for certification processes. A properly designed certification process must include a clearly timed project plan. If there is not enough time to properly evaluate and certify the election technologies, other areas requiring preparation and overall management may also be falling short.

Certification is no more than rubber-stamping an election. A fear often raised in established democracies is that certification procedures merely rubber-stamp certain election technologies and the electoral process they are used in. It is true that some certifications can be superficial, and fail to add real quality assurance to the certified system. To ensure that certification provides real value, it is best to develop an understanding of what a given certificate covers, and how it was obtained.

Certification is an insider business anyway. In some industries, the relationships between vendors, evaluation and certification bodies are very close and not regulated by a strict code of conduct. In the area of elections, the general public and the media have a high level of interest in all parts of the electoral process. To ensure that this interest does not become corrupted, all parties involved in the certification of election technologies must adhere to a strict separation of power and codes of conduct. The task of the regulatory framework is to avoid any situation in which accusations of insider business would be able to fall on fruitful grounds.

Certification is not applicable to 'our' kind of election technology. The certification of election technologies originally stems from the use of electronic voting machines: a single machine would be evaluated and then certified. The vendor would then issue a statement of compliance that all similarly produced machines would meet the same criteria as the evaluated machine. EMBs that use a different form of election technology—Internet voting in particular—argue that their systems consist of a single unit, and hence certification would be pointless.

Our country is too small for certification. Establishing a functional infrastructure for certifying election technologies requires additional expertise within a country. In particular, essential parts of the certification process—such as drafting and defining specifications and requirements or issuing the certificate—should be performed by domestic experts. This does not mean that other stakeholders or international experts cannot support the process. If enough time and resources are dedicated, any electoral context can develop the expertise needed to conduct a quality certification process.

One cannot be sure the running system is the one that was certified. The guarantee that the election technology in use is the one that has been certified has to rely mainly on organizational measures. Recent research in this area is intended to make this an issue of the past, but it will take considerably more time.

Certification might fail. If certification fails, it can be assumed to do so for good reasons. Rather than perceiving this issue as criticism, detecting shortcomings of election technology ahead of their use should be seen as protecting democratic principles. It is best to have an established law or guidelines that address the possibility of such a failure. This protocol should be made public ahead of the elections in order to avoid any surprises or unwanted complaints and criticisms if a failure occurs.

Should election technologies be certified?

Discussions about introducing election technologies usually include how to ensure that the technology delivers the required functionalities; this is particularly true when transitioning from paper-based systems to electronic ones, because one cannot see, touch or feel bits and bytes. Many call for certification to solve this 'black box' problem, but most of the time it is unclear what this certification should entail. Notions of certification mainly encompass an evaluation of the technology in question by a competent external actor, which in turn will build trust in the election technology. Further aims are to be inclusive (include opinions other than the ones responsible for the system), build a secure system (by being reviewed by experts in the field) and provide accountability (that the technology performs as planned). As a result, certification becomes the do-it-all answer to all kinds of concerns

related to the introduction of election technologies. Further reasons to carry out certification can include a legal requirement or the need to verify the correctness of an election outcome.

All of these approaches involve third-party involvement. Such involvement can be grouped into three categories:

1. *Expert opinion*: statement by a highly regarded external person or company about a system's properties. This is the most flexible category, and the opinion is valued by the contracting authorities or the general public. Such documents are relatively free in format, and their conclusions should be interpreted in the context of the author's background. The definition of an expert is subjective and relative, and one expert's findings can always be contradicted by those of another.
2. *Review* (or assessment, audit, evaluation, inspection, testing, verification): the process of verification by competent and independent bodies to determine the extent or level of assurance or fulfilment of particular properties. These typically analyse the election technology against a set of requirements that is defined and/or prescribed by the contracting authority, recent academic literature, relevant legal documents and/or international standards. The methods by which these reviews check the system against these specifications are flexible, as is the associated reporting. Rather than a yes/no decision, indicating whether the system complies with the requirements, reviews (usually conducted by independent third parties) assess the vulnerabilities and associated risks.
3. *Certification*: a systematic process (carried out by an accredited third party) to evaluate whether a given election technology satisfies systematically established standards and/or legal requirements. This process may include hardware and software, as well as operational systems, management processes and personnel. Both the requirements and the evaluation are derived or conducted systematically. In addition to a report, a certificate attests to the achievement of compliance with required standards.

Australia: When the Australian state of Victoria launched an end-to-end verifiable kiosk-based voting system called vVote in 2011, different developer teams initially reviewed each other's code. In March 2014 a third-party evaluator, the DemTech Group, evaluated the entire system. In an effort to create transparency, the evaluation report was published on the Victoria Electoral Commission's (VEC's) homepage, accompanied by a detailed response from the VEC. No certification was sought by the VEC.

For more details about this case see Annex A.

Table 2.1. Models of third-party quality assurance

	Checked against requirements	Accredited third party	Changes after completion	Result
Expert opinion	No	No	Yes	Report
Review	Yes	No	Yes	Report
Certification	Yes	Yes	No (or very limited)	Report/certificate

While certification might be the end goal of many efforts to evaluate compliance, it is also the most complex and time consuming. Where limited resources are available, reviews might be more appropriate, even though they do not deliver the same level of assurance regarding the quality of the system in question. Other coping mechanisms might be to limit certification to the most critical parts of the system analysed, which still helps improve its overall quality.

Other reasons for reduced or different kinds of approaches to certification can be very complex systems that would be very hard to document and analyse, or just-in-time systems designed to answer concrete needs within a short timeframe. In such cases, individual processes might be preferred, although comprehensive approaches should remain an intermediate goal.

Certification might not be necessary for all IT systems used in an election, in particular when they are used for non-critical elements such as managing meetings and their minutes, and other transparent and easily approachable election technology modules.

All of these efforts should be clearly differentiated from domestic or international election observation activities. Election observers are usually active for several months to a couple of weeks before election day and stay for a few days to several weeks afterwards. Election observers look at the whole electoral context in which an election takes place, including, but also going far beyond, the technologies and processes that are subject to certification. Election observers cannot be perceived as equivalent to a certification, or even as providing a structured review of election technologies. Nevertheless, observers will be very interested in learning from those involved in reviews or certification, and will assess their findings.[1]

This Guide focuses on a framework for review and certification, and provides guidance on designing a process for third-party analysis of a given election technology. It aims to support EMBs in their decisions and help others understand and contribute to such efforts.

[1] For more on this, see OSCE/ODIHR (2013).

Risks

Examining election technologies—especially in conflicted contexts, or where there is a lack of trust in the electoral authorities—can become a crucial part of preparing for elections. This focus, in turn, can put a lot of pressure on a certification process, during which weaknesses, vulnerabilities and problems might be identified that need to be fixed before the technology can be used.

Problems can also occur in the certification process that have little to do with the technology itself. For example, certification takes time (which may be scarce), and if a vendor is inexperienced in writing documentation in a suitable format, this can cause delays. The overall complexity of the election technology can create additional problems within the process that have nothing to do with faults in the product. Limited communication processes, such as closed-door policies and the provision of only passive information to the public, may also contribute to rumours and unhappiness among some electoral stakeholders.

Vendors and even certification bodies can also create artificial hurdles in this process by requiring the persons conducting the review/certification to sign very restrictive non-disclosure agreements (NDAs). While NDAs are a standard prerequisite to prevent others from disclosing business secrets, they violate the democratic ideals of providing transparency and accountability to all electoral stakeholders, including the general public. NDAs can produce a consequent need to keep documents related to the evaluation procedures secret, which can create distrust. An acceptable balance should be found between transparency and protecting the vendor's intellectual property rights and system security protocols, since both are essential elements of the process.

Austria: In Austria, the final evaluation report of the certification of an internet voting system was not made public, and representatives of parties could review it on only one day in a dedicated room. This led to heavy public criticism of the process.

For more details about this case see Annex A.

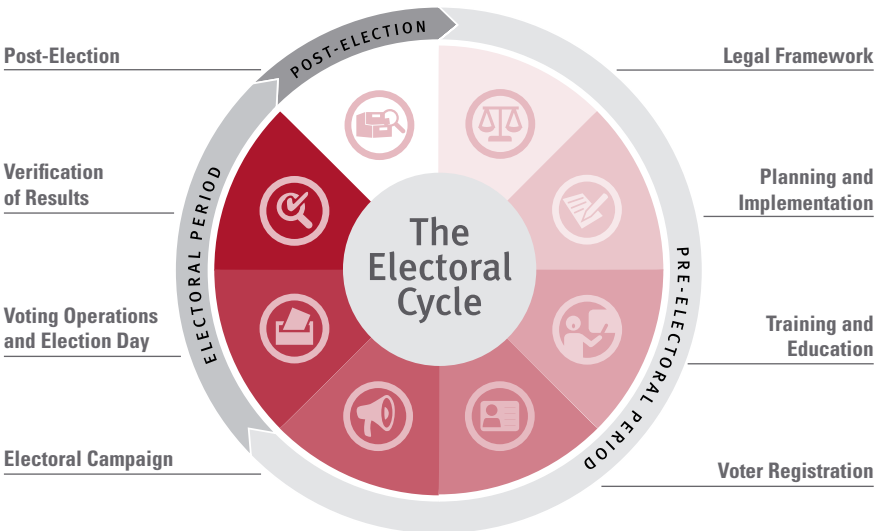
CHAPTER 3

What Can Be Certified

Components of the electoral cycle

Elections are best described using the electoral cycle approach. Figure 3.1 depicts the three main phases of the electoral cycle.

Figure 3.1. The electoral cycle



Source: International IDEA

At the beginning of a certification process, the questions are always the same. How can the EMB be sure that an election technology can be safely deployed? How can it take responsibility for technology and processes? The technology and the surrounding processes will be subject to public scrutiny and validation; they cannot be considered in isolation. For example, all safety-critical systems come with a set of (digital) keys that must be generated and administered. Since these processes include humans as well as technology, any quality assurance measures will need to include technology as well as the related administrative processes.

Quality assurance methodologies can increase the confidence of all stakeholders, for example, through extensive testing, third-party evaluation, gradual roll-out to only a small fraction of the electorate or simple redundancy measures, such as alternative voting channels or printed poll books. As EMBs have increased their ability to use ICT, many have created their own information technology (IT) departments, with best practices emerging as regards quality assurance. International standards help harmonize the technical specifications of products and services, and provide assurances about their quality.

Given the complex nature of election technology, the quality assurance process needs to evaluate a combination of operational procedures and technical designs to determine the risk of weaknesses in operational practice and ICT controls. Vulnerabilities in any systems or components can compromise the trustworthiness of the security mechanisms that rely upon them, and should be highlighted during the quality assurance process.

It is important to note that quality assurance methods will lead to an improvement of technology and processes, but it is unreasonable to assume that these methods will uncover all weaknesses or guarantee perfection. The quality assurance process relies on several assumptions (for example, that access controls are strictly regulated and implemented, or that a computer's hardware is not compromised) that need to be true in order for a system to work correctly.

Technologies

Election technologies run on computers that may be connected through private or public networks such as the Internet. Each computer consists of hardware, firmware, an operating system and the election software.

Firmware is programme code stored within the read-only memory (ROM) of a computing device that enables other software programs to run on it. It is programmed during the manufacturing process, and may be updated by a user or adversary. Firmware is usually developed by the original manufacturer and occasionally by independent companies. Manufacturers often release updates to firmware to fix bugs, patch vulnerabilities and support new

hardware. Unauthorized modification of the basic input/output system (BIOS) firmware system by malicious software presents a significant risk, given its fundamental role within the computer architecture.

Hardware comprises all of the electronic components of any computer, both internal and external. Its functions are divided into four main aspects of data handling: input, processing, output and storage. External hardware devices connected to the computer are usually called peripherals. Peripheral devices include input devices (such as a keyboard or mouse), output devices (such as printers and scanners), storage devices and communication devices.

The **software** provides the instructions that tell the computer to perform a specific task and prescribe how it is to be done. The two main categories of software are *the operating system* that runs the computer and controls all of its operations and the *application software* that allows users to perform specific tasks on the computer. The operating system has three main functions: (a) manage the computer's resources (central processing unit, memory, disk drivers and peripherals), (b) establish a user interface, and (c) execute and provide services for application software. Application software can be applied to perform a task or to solve a particular problem. EMBs usually invest in a mix of custom-developed election software that is specifically tailored to their needs and standard task-oriented software packages.

Election technologies can either be *stand alone* (a computer system or device that is used in a small-scale context, plus devices that are connected only to that system, and do not share information resources with any other system or device) or *interconnected* (a system that is connected to other IT systems in order to share information and resources). Any component of an interconnected system, when not appropriately protected, may compromise its integrity. All of these technologies are embedded in organizational and administrative processes, which involve commissioners, election officials, poll workers, voters and other stakeholders.

Throughout all phases of the electoral cycle

Processes

Contingency plan

The contingency or continuity plan is a list of contingency measures and policies to ensure the continuous operation of the electronic election system in case of delay, breakdown, failure or 'disasters'. As with most automated systems, there is usually a legally mandated system wherein the EMB is required to develop—and, in the case of trigger points, operationalize—the continuity plan to cover possible risks in the overall system. Since this system

usually involves a fail-safe mechanism that is activated by predetermined triggers, the certifier must ensure that the plan adequately addresses critical areas. However, the political nature of elections, and the concomitant activation of a new process, will require transparency and broad acceptance of various stakeholders in order to avoid any semblance of bias or mistrust. Thus processes for transparency such as the publication of contingency plans, and the involvement of competing parties early on and upon activation, are necessary. Elements subject to quality assurance measures may include the document describing the strategy, the process and the overall testing of the fail-safe mechanisms, such as generators, battery packs, extra machines or the presence of ready support.

Internal auditing mechanism

Election technologies require a built-in audit mechanism to determine early on the accuracy of results in the critical stages of the system. In certain jurisdictions, a parallel or random audit is conducted to ensure that the whole system functions accurately. Any error or discrepancy usually results in a root-cause analysis, and, if warranted, the activation of the fail-safe plan. Transparency is one of the most important criteria in audits, whether done internally or through third parties. The range or scope of audits should likewise fall within acceptable sampling methods. Auditing mechanisms should be verifiable and produce accurate results in a timely manner. Other criteria may include the integrity, security and auditability of the chosen process.

Technology components

Vote service portals

Vote service portals provide voters and candidates with a variety of election-related information, including about candidates, parties, voting eligibility and election results. Since the correctness of the information on such portals is crucial for the success of the electoral process, the software should be subject to review, in particular for load balancing and as part of stress tests.

Electoral administration systems

The electoral administration system is the essential information management tool for the whole electoral process. Ideally it includes all forms of electoral information, from calling the election through to the swearing-in of the new government. Due to the system's sensitive nature, and to avoid errors, end-to-end (E2E) testing is crucial for the integrity of the election. Further assessments should include an analysis of how vulnerable the system is to risks such as cyber attacks.

The pre-election phase

Processes

Boundary delimitation

This is a process to create constituency boundaries following previously established patterns that may rely on geographical data, population data, other social features (for example, ethnic/linguistic/religious composition and history) and electoral data (for example, proportional or majority representation, appropriate number of seats). Updates are needed on a regular basis, particularly for majority systems, and such modifications may raise political concerns of boundary biases (gerrymandering). Several aspects must be taken into account in order to ensure a fair distribution of electoral districts, including representativeness/non-discrimination, transparency, equality of voting strength and stability. Due to the political nature of the boundaries, external review is desirable in order to ensure unbiased decisions, but this may be difficult to achieve.

Electoral education

Electoral education aims to enhance the overall awareness and skills related to electoral procedures. It consists of voter education, training for poll workers, and similar activities for other stakeholders (for example, media, political parties and civil society).

Registration of political parties and candidate nomination

Legal regulations and relevant procedures determine how to decide which entities are eligible to be political parties. These regulations affect public rights (for example, funding) and duties (for example, transparency and internal democracy). Candidate nomination takes place shortly before an election, and can either be linked to previously registered political parties or allow independent candidates. A formal declaration of candidates for a given election is needed, and should be published according to a clear time schedule. The advance publication of candidate names can help to show that no bias or manipulation has taken place.

Oversight of media coverage

Legal regulations may establish temporal (that is, quotas) and substantial (that is, neutrality) limitations for electoral media coverage, with the aim of guaranteeing a fair electoral campaign period. Such rules may apply to both private and public broadcast stations and the printed media. Democratic elections need an overall balanced and pluralistic media framework. External monitoring and review can provide additional transparency for an electoral process, and is particularly valued by election observation missions.

Election logistics

Election logistics include operational processes for a public service that needs to be delivered within an extremely short period of time. Since there is no room for delays or mistakes, logistics become crucial. Examples include planning how to produce, maintain, distribute and use electoral material; human resources management; budgeting, procurement, communications, training and evaluation strategies.

Oversight of campaign financing

EMBs are often responsible for monitoring how political parties spend and receive funds from public and private sources. Such funds may apply to campaign activities as well as to regular party functions (for example, human resources, premises). The legal framework specifies detailed guidelines, limitations and relevant sanctions to ensure transparency about the ways in which candidates and parties fund their campaigns, and respective expenditures are examined. IT systems can be used to make this data public.

Technology components

Voter registration

The voter registration process aims to build an electoral roll that includes all people entitled to vote in a given jurisdiction. Voter registration can either be conducted on an ongoing permanent basis, or only for specific elections. Passive (automatic) or active (on-demand) approaches can be used. Data privacy issues need to be considered when creating and maintaining the electoral register. Specific voting channels (for example, Internet voting) may need supplementary voter registration steps.

The voter list must be frozen at a specific point in time before election day, and a public entity should be responsible for establishing the final list. Citizens and other stakeholders overlooked by the law may request amendments. In contexts of distrust, it is useful for external parties to analyse and review voter registration components.

The election phase

Technology components

Voter authentication

Voter authentication on election day can be supported by additional election technologies such as biometric fingerprint readers and/or electronic poll books, which help track the participation of individual voters in the election.

Biometric technologies help to verify the identity of a particular voter as well as their access to a designated voting centre.

Electronic voting machines

Electronic voting machines were the first election technology to be certified and for which related concepts have been developed. While it is generally considered to be necessary to certify them, formal requirements are still lacking and have to be drafted for each context of use. There is a general consensus that voting machines without voter-verifiable paper audit trails (VVPATs) have much higher certification requirements than machines with VVPATs.

Internet voting

Technologies that allow individuals to cast their vote via the Internet are the most challenging and complicated election technologies to evaluate and certify. Due to the Internet's technical properties, assumptions about the operating context need to be carefully evaluated in order to realize a high level of security.

Ballot scanners

The least complicated voting technology is used for vote casting or counting of paper ballots. Ballot scanners provide a means of reconciling the number of votes cast on paper with the number of votes tallied by the electronic system counting them. The built-in paper trail makes these systems easier to verify than electronic voting machines. Nevertheless, certifying ballot scanners, including considerations about recognition failure rates, is significant for the perceived accuracy of the results.

The post-election phase

Processes

Data retention

Individual voters' data must be protected. This data includes electronic ballots that need to be prevented from being accessed past a certain period after the electoral results have been determined, and may stipulate disaster recovery.

Different jurisdictions may require separate data retention policies for electronic and paper data. Depending on the electoral process and the corresponding election technologies used, there will be a system for safekeeping, storing and archiving the physical or paper resources used in the election process. Similarly, the EMB will need a system that adequately addresses requirements

for storing and safeguarding electronic data, including the hardware and software for data storage as well as physical security of data storage areas.

Technology components

Result transmission system

Electronic transmission in the context of automated election systems conveys data in electronic form from one location to another. The electronic results can be generated by voting devices such as voting machines or Internet voting systems, or be entered manually at a polling station. A centralized system then consolidates the results, and depends on them having been correctly transmitted. Therefore the transmission of results at all levels should be reviewed during the certification process.

Tabulation system

The tabulation system aggregates the results and assigns mandates according to legally defined and often complex procedures and formulas. Such systems should be reviewed for accuracy and correct implementation of the related legal framework.

Netherlands: At the request of the EMB, a third-party testing company was contracted to assess the result tabulation and seat allocation software against its technical specifications and requirements. Academic experts assessed the legal correctness of the technical specifications.

For more details about this case see Annex A.

Publication of results

In the final step of any election, the results are published on the election portal, together with information that helps the stakeholders understand the final results. These systems are often integrated into public election information websites. Due to the public's high interest in timely results, it is important to stress test result publication systems to make sure the system is able to withstand high demand access and to make sure that the presented data cannot be manipulated.

CHAPTER 4

Quality Assurance Framework

At first glance, it seems that certifying election technologies is similar to certification processes in other sectors and industries. Yet there are significant differences that make the certification of election technologies more complex.

Certification in many sectors builds on existing, well-defined national or international technical standards that reflect applicable legal requirements. Such standards are developed for large markets by international or regional standardization bodies with well-established procedures. Moreover, such standards are finalized and stable long before a certification process starts, and even longer before a certified system is used for the first time. It is also clear what the competent certification body is for each standard.

USA: The United States Election Assistance Commission does not test electronic voting and counting equipment systems itself, but provides accreditation to testing labs (voting system test laboratories or VSTLs) that evaluate voting systems, voting devices and software against the voluntary voting system guidelines to determine whether they provide all of the basic required functionality, accessibility and security capabilities.

For more details about this case see Annex A.

In general, certification cycles are long and the target dates can change. If there are delays, the worst that can happen is that a product will take longer to enter the market. If standards and requirements change, existing systems are not expected to comply at once; transitional periods often span several years.

Certifying election technologies

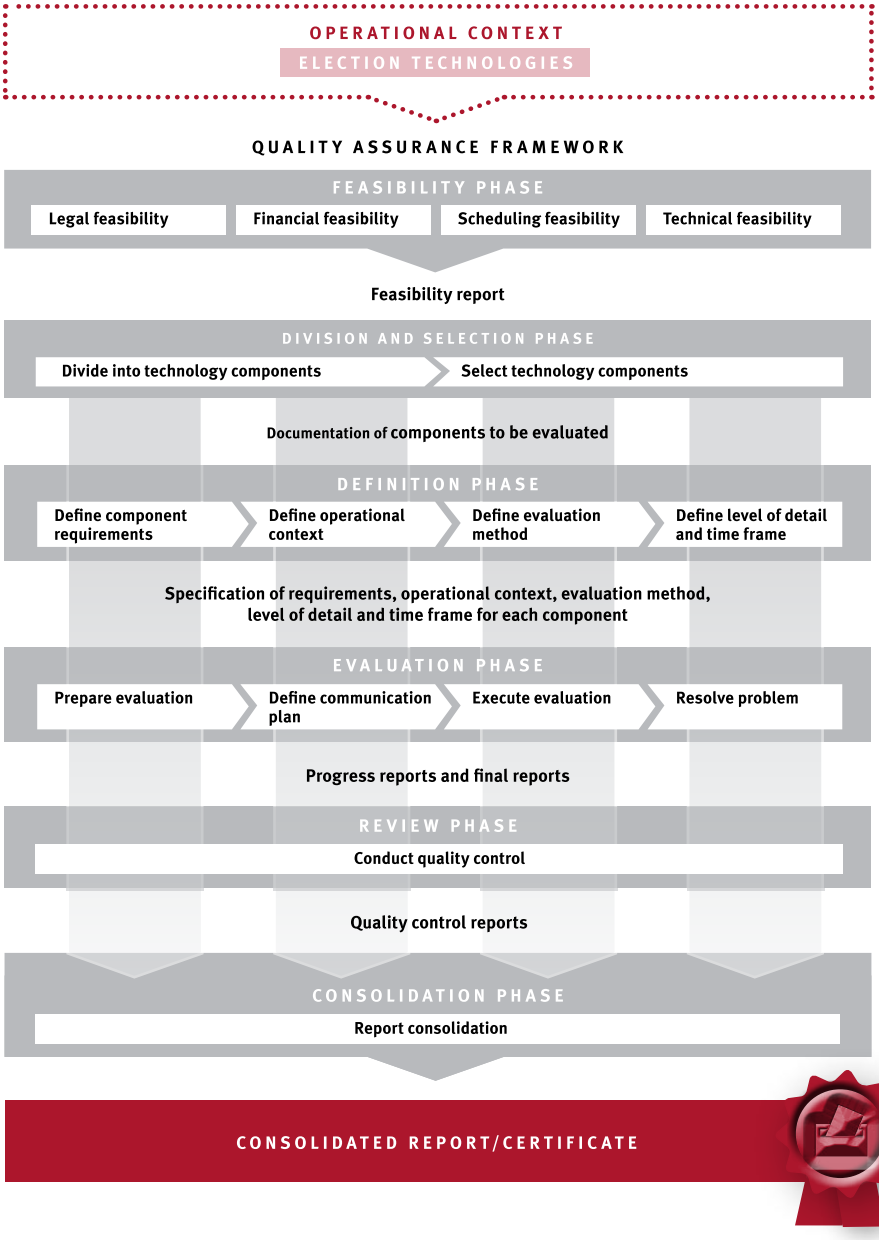
For elections, the situation is entirely different. Election dates are fixed, and all election technologies must be available and operational by a specific date. There is no standardization body to develop international technical standards for election technologies; each EMB must develop its own applicable standards and requirements and assure compliance. Developing standards and requirements must take national and international legal frameworks into account that are often not designed to provide technical guidance, which makes it hard to derive clear technical requirements against which a certification can be conducted. The International Organization for Standardization published ISO/TS 17582:2014 for electoral organizations, however this relates primarily to quality management rather than product certification.

To help EMBs plan and implement certification processes, this section describes a quality assurance framework that summarizes best practices. It can be used to certify election technologies and render them more transparent.

The framework

This section presents the Quality Assurance Framework, which provides a comprehensive overview of the steps that may be performed when assessing the quality of the election technology components of the electoral process. The electoral process consists of several steps, as discussed in Chapter 3, including voter registration, party registration, electoral logistics, vote counting and tools to provide initial results to the media. All such activities—organizational or electoral, with and without ICT support— can undergo quality assessment.

Figure 4.1: Overview of the Quality Assurance Framework for election technologies



The framework, as depicted in Figure 4.1, describes the different phases and their deliverables. EMBs may find this framework useful for planning a quality assurance process and estimating the kinds of resources needed to complete it.

The discussion that follows refers to the part of the electoral process to be evaluated as the *election technologies*. It is assumed that precise requirements and system design documents are available. The Quality Assurance Framework is a methodology designed to evaluate an election technology system in a sequence of phases:

1. feasibility;
2. division and selection;
3. definition;
4. evaluation;
5. review; and
6. consolidation.

Feasibility phase

Definition: The feasibility phase involves identification of the general scope of the quality assurance process and determination of the legal, financial, scheduling and technical feasibility. Quality assurance mechanisms can, if used correctly, detect errors at early stages, and thus improve the quality of the election technology.

Activities

- *Legal feasibility*: The conduct of elections is generally regulated by laws and acts, which might influence the certification process. For example, legal regulations might determine the procurement of evaluation and certification bodies, which in turn might impact on other parameters. The feasibility study should verify that there is no conflict of interest.
- *Financial feasibility*: EMBs' financial resources are limited. Since evaluating and certifying different aspects of the election technology might become cost intensive, cost-benefit analysis should be an integral part of this phase.
- *Scheduling feasibility*: The certification process may be time consuming. The feasibility study should take into consideration legally prescribed time frames, the time needed for decision-making, the time until the next election, and how the certification process should be regularly conducted to ensure timely completion.
- *Technical (operational, infrastructure) feasibility*: The EMB evaluates whether its operational and infrastructure capabilities satisfy the minimum requirements for the quality assurance process.

Resources: The EMB or a designated technical advisory committee is responsible for managing this process.

Output: The feasibility report should indicate scheduling constraints, legal and technical requirements, and available financial resources.

Division and selection phase

Definition: The division and selection phase defines the overall target of the evaluation and divides it into the parts, processes and components to be evaluated. The target may be the entire election technology system or elements of it, such as the process of staffing a polling place, or the component that implements the user interface or cryptographic protocol. The objective of this phase is to decide how to divide the overall system design into components—which may include protocols, hardware, software and processes—and select those that will be evaluated.

Activities

- *Divide into technology components*: Election technology systems are usually complex and need to be evaluated from different perspectives. An Internet voting system, for example, contains communication mechanisms that should be analysed in terms of its security, and a user interface that should be analysed with regards to usability. Some voting systems provide mechanisms for individual and universal verifiability, and their reliability depends on voters checking their cryptographic receipts. Another example is a digital voter registration system that is used to cross voters off the electoral roll after voting. Voter registration systems must be easy to use, and should be designed to easily recover from unforeseen problems such as system failures.
- *Select technology components*: Taking into account the results of the feasibility study, EMBs should prioritize the system elements to be evaluated. It is in an EMB's interest to allocate resources in a way that maximizes quality assurance. For example, the EMB could prioritize components that are mission critical and/or have specific legal requirements.

Resources: During the division and selection phase, the EMB identifies specific components to be evaluated.

Output: A list of precisely described and documented components to evaluate.

Definition phase

Definition: Based on the results of the previous phase, the definition phase identifies the component requirements, defines the operational context and identifies the evaluation method, level of detail and time frame for the evaluation.

Activities

- *Define component requirements*: The EMB derives requirements based on the results of the feasibility study and according to best practices and expert advice. It should also consider (and be aligned with) requirements for interdependent components.
- *Define operational context*: The EMB identifies the assumptions and unique circumstances of the election settings. For instance, evaluating an election communication infrastructure that utilizes multiple relay steps—such as from central headquarters to regional offices, an area office, the electoral district and the local voting station. This evaluation process requires more resources than a flat communication infrastructure that allows direct information flow and control from the central EMB to local electoral offices, because it has more failure points.
- *Define evaluation method*: The EMB reviews suitable evaluation methods, and defines new ones if necessary. These might include well-established methods, for example as outlined by the Common Criteria Protection Profiles, ISO 9001 or country-specific standards.
- *Define level of detail and time frame*: The EMB defines the scope of the evaluation, indicating the level of detail at which it is to be conducted. During this phase, it should also specify the deadline for completion.

Resources: During the definition phase, the EMB is responsible for specifying the evaluation tasks.

Output: The requirements against which components are to be evaluated, the specifications of operational context in which components will be used, the choice of an evaluation method, as well as the specification of evaluation requirements in terms of the level of detail and time frame.

Evaluation phase

Definition: The certifying agent or body, using the parameters set and the assumptions agreed upon, systematically determines the degree of compliance with the standards and scope defined. If the evaluation identifies any problems, this phase may be used to conduct corrective actions.

Activities

- *Prepare evaluation*: The EMB initiates operational meetings, introduces key personnel and coordinates task assignment.
- *Define communication plan*: The EMB and the evaluator agree on a communication plan that includes the establishment of a communication structure, alternative means of communication and escalation procedures.

- *Evaluation execution*: The evaluator produces the designated output as stated in the scope of work.
- *Resolve problems*: If the evaluator finds issues or irregularities during the evaluation, it is the EMB's responsibility to fix these problems, which may entail making changes to the component under evaluation.

Resources: This phase is a joint effort between the EMB and the evaluators.

- *Evaluators*: Prior to the evaluation phase, suitable evaluators need to be identified and recruited.
- *Management*: As part of resource management, it is important to agree on the terms of the evaluation in advance. Based on the results gathered during the definition phase, the contract with the evaluators must precisely define expectations and time requirements, as well as the provision of documents and deliverables (such as evaluation reports). The evaluator must closely and regularly coordinate with the EMB during this phase.

Output: There are two major outputs at this stage: progress reports and final reports. The progress reports describe the findings to date, and may suggest corrective measures. The schedule for submitting progress reports should be agreed prior to the evaluation phase. The final report's details summarize relevant findings, corrective measures and recommendations.

Review phase

Definition: This step is used to revisit the findings documented in the reports produced during the evaluation phase. This phase is optional: it will not evaluate components, but rather check the evaluation reports for consistency and quality. Reviews resulting from this phase are not to be confused with the term 'review' introduced in Chapter 2.

Activities

- *Conduct quality control*: The EMB creates a quality control team responsible for reviewing the reports from the previous phase. The team must submit a report confirming that all evaluation activities were adequately completed.

Resources: The quality control team responsible for the review phase is usually comprised of third-party reviewers. The team may also involve quality assurance reviewers who reassess the initial findings of the evaluators.

Output: The output of this phase is a quality control report.

Consolidation phase

Definition: The consolidation phase combines the findings of the individual evaluation reports to create a single quality assurance document.

Activities

- *Report consolidation*: All output reports from the previous evaluation phase are merged into one unified document that communicates the result of the overall quality assurance process.

Resources: The EMB is responsible for assigning external resources to complete this process.

Output: The output of this phase is a consolidated report, which can be used to prove compliance with specific standards in order to issue a formal certificate.

Summary of the quality assurance process

The Quality Assurance Framework provides EMBs with a means to evaluate election technology within a specific operational context. Depending on the evaluation methods utilized and the resulting evaluation reports, individual components may comply with specific standards, in which case accredited certification bodies may award certificates.

CHAPTER 5

Deriving Requirements

From legal to technical

Constitutional law is usually the expression of a country's culture and identity. Consequently, election regulations differ from one country to another, and they are always enshrined in constitutional and basic laws. In principle, such normative requirements—both the high-level concept and the detailed format—provide guidance for conducting elections throughout the electoral cycle. For certification purposes, this framework can be considered the legal requirements.

When constructing and evaluating election technologies (and their components and processes), the legal requirements have to be transformed into technical requirements the certifier can use for the evaluation.

Switzerland: Each canton using electronic voting needs to get approval from the Federal Chancellery. This approval is based on tests in the given context monitored by the Chancellery.

For more details about this case see Annex A.

Translation into technical requirements

Determining technical requirements requires close cooperation and dialogue between legal and technical experts. While technical requirements may need to identify the context in which they are to be implemented, legal requirements may also be shaped, nuanced and weighted when deployed. Therefore, understanding legal ductility is essential for developing proper technical requirements.

Legal ductility: Acceptable margin of appreciation when determining the meaning of legal terms.

Legal latitude: Method of providing a fair solution when contradictory principles apply to a given case.

Legal ductility may apply to at least two different scenarios: legal cultures and legal interpretation.

First, the same legal principles may convey different meanings depending on the socio-cultural context in which they are used. Secrecy, for instance, is a clear international commitment, but each country may interpret it differently (for example, using voting booths is not mandatory everywhere).

Second, the same legal principle may convey different (and even contradictory) meanings depending on the means of interpretation, even within the same country and with similar socio-cultural patterns. Context-based and result-oriented interpretations are standardized methodologies of analysing legal principles; both help resolve legal discrepancies fairly. Case law also provides legal inputs that directly shape the meaning of legal principles.

Contradictory legal principles may be weighted so that the main legal goal is achieved even though none of the components of the legal system is fully satisfied. Such a legal latitude may take place at a constitutional or legislative level (for example, postal voting, individual vs. territorial representation in parliament) or in court, but practitioners can also extract the relevant trade-offs comparing existing legal rules with the needs of a real situation.

Once defined, the legal framework is subject to technical requirements that not only further develop it but also constantly reshape its content through normative modifications and recurrent case law adaptations. Thus technical requirements, which will face several barriers during their implementation, also represent important inputs for legal updating. Legal and technical issues have mutual interactions that are based on reciprocal, rather than unilateral, patterns. Reusing existing technical solutions represents another clear example of reciprocal dialogue between the legal and the technical side. When translating legal terms into technical requirements, solutions that have been implemented in other contexts could be used if they prove to have addressed similar problems.

Technical requirements used as a basis for certification are not only derived from the current legal framework. They can also incorporate aspects of non-domestic legal frameworks or technical requirements that might become legislation or serve as particular features of the election technology. Incorporating requirements that are out of scope of domestic legislation

might, for instance, be interesting if certification is to be valid for a longer period of time.

Consideration of the context

EMBs should not expect to find a global certification procedure that would be valid everywhere. Although some common patterns might be highlighted, each country is likely to need tailored certification solutions that will take into account its specific socio-political, legal and technical needs. Moreover, each electoral jurisdiction represents a context for which the technical requirements and overall certification process should be adapted.

The technical requirements of different components and processes might not be implemented unconditionally for all application settings. Consider, for instance, the evaluation of a cryptographic key distribution scheme. The number of entities with which a secret cryptographic key will be shared affects the extent to which vote secrecy is enforced, yet it does not impact the usability of the voting interface—for this, voters' technical affinity is important, but this does not impact on the degree to which vote secrecy is enforced.

Technical analysis can only assess the risks; public authorities need to decide which threats and risks are acceptable when conducting elections. Fulfilling technical election technology requirements depends on the context of (the expected) threat scenario. Here, the concept of the separation of duty is helpful. It can be expressed using the so called k-resilience value, which indicates how many entities need to be compromised to jeopardize the integrity of the election (for more details about k-resilience see Annex B).

Requirement catalogues

When deriving technical requirements, EMBs do not have to start from scratch; they can build upon previously established requirement catalogues, such as the following.

ISO standards: Several ISO standards capture requirements for election systems, for example ISO/TS 17582 quality management systems and several common criteria protection profiles. Despite the practical relevance of several protection profiles (for example, PP-CIVIS (2006), IEEE (2005), Lee et al. (2010), Karokola et al. (2012)), most do not consider verifiability, a requirement provisioned by many legal frameworks.

Region-specific requirements: Based on legal provisions, several nations and regions have determined sets of individual technical requirements. For example, the Council of Europe (CoE) released their Recommendations

Rec(2004)11, which covered 51 technical requirements for electronic voting; Germany captured requirements for voting machines in the Voting Machine Ordinance (1975); France released a legal decree in 2003 (Ministère de l'intérieur de la securité intérieure et des libertés locales, 2003); the United States of America recently released its Voluntary Voting System Guidelines in version 1.1 (EAC 2007); and in 2014 Switzerland specified requirements for the conduct of remote electronic voting, including the requirement to give voters in some cases the ability to individually or even universally verify the vote. Region-specific requirements might be a good way to customize the certification process to a particular context. Yet weak local developments may not fit international criteria.

Private associations: A number of private associations have released requirement catalogues for running technically supported elections. Both the International Association of Cryptologic Research (2015) and the German Gesellschaft für Informatik (2005) have developed a list of technical requirements for remote electronic voting. The Institute of Electrical and Electronics Engineers has developed a standard for voting equipment, with the goal of facilitating the data flows and election processes of technically supported elections. While these technically driven approaches are certainly a good starting point, their implementation might find unexpected barriers due to a lack of realism or context failures.

Research literature: The scientific community has also addressed the challenge of deriving technical requirements for electronic voting. Yet the research literature might not always be a complete solution. Technical academic papers are often tailored toward fine-grained interpretations of technical requirements, perhaps neglecting other requirements: for example cryptographic schemes that deploy coercion resistance as a strong form of vote secrecy without considering usability. In such cases, research papers would essentially serve as aids rather than requirements catalogues. However, some academic papers could also set up a complete new requirements package, which might help stakeholders implement certification procedures.

Further information about the research literature focusing on the derivation of technical requirements is available in Volkamer (2009) and Neumann and Volkamer (2014).

CHAPTER 6

Planning

With the help of the Quality Assurance Framework, it is possible to structure the certification process for electoral technologies. Yet further considerations are necessary when implementing such a process. This chapter provides guidance on the planning, timing, and overall transparency and communication of the certification process.

Planning the certification process

As with any important activity that needs to be managed properly and effectively, prior planning is essential to its success. The following concerns should be factored into the certification project plan:

1. selecting the certification body, including the selection criteria;
2. identifying the minimum standards and preferred methodologies (if any) to be used;
3. identifying the minimum certification requirements for compliance;
4. identifying the scope of work to be covered by the certification project;
5. estimation of costing or budget for the project, including such detailed items as the cost of the certification service, and other incidental and operational expenses;
6. identifying manpower requirements for putting together review/validation teams, especially when consolidating individual certifications of different components of an entire system;
7. the time period allowed for the project, especially immovable dates that are prescribed by law;
8. scheduling of reporting requirements;
9. transparency or communication strategy, including the level or degree

of transparency that will be implemented, which information may be disclosed, and how to handle different groups of stakeholders (whether critics or active supporters) if there is a failure of certification; and

10. overall responsibility for the project, including specific identification of responsibilities and accountabilities.

Significance of the selection of a certification body

Since only an accredited body can issue a certificate, selecting which persons or entities are entitled to conduct certification procedures is a critical step. One should consider that, from a layperson's perspective, the content of the reports and the subsequent certificate will be meaningless due to its technical profile. Trust will only be enhanced if the certification bodies provide sound credentials of their professionalism, and if that guarantee is directly linked to the criteria used to select such entities. In short, the selection of certification bodies goes far beyond a purely technical decision, and is linked to citizen confidence, public interest awareness and the institutional separation of powers.

Who is entitled to conduct a certification?

The first requirement is to make public the criteria used to select certification bodies. These criteria should be established well in advance, and could be submitted to appropriate hearings with relevant stakeholders. The context is likely to which criteria are really needed; different scenarios might be foreseen.

For instance, if an overall consensus guides the implementation in a given country, EMBs could easily find well-known local and/or international experts. Their professional background would be enough in such cases—no further formal qualifications would be needed. Standard national or international practice should be enough. On the other hand, qualified certification agencies could be helpful. The criteria used to determine the nature of a qualified certification agency would have to be established by law or by EMBs. Such criteria should be objective and independent of discretionary decisions. Self-certified or self-proclaimed 'certifiers' should not be allowed.

Philippines: a committee, independent of the EMB, is mandated by law to certify the automated election system (AES) to be used on election day. This certification is to be done through an evaluation by an international certification entity (ICE). The list of authorized ICEs is provided to the EMB by an advisory council, a body that is created by law and composed of representatives from different sectors of society. This council is presumed to have knowledge and expertise of ICEs.

For more details about this case see Annex A.

Who contracts (and pays) the certification body?

Once it is established which persons and/or entities can conduct a certification process, the legal framework should determine how to select one or more of these bodies. Different scenarios are possible. For example, the selection of a given certification body could depend on the vendors themselves. EMBs could only use products that have been previously certified by one of the accredited certification bodies enlisted to do so. However, this relies on each vendor's preference for which certification body is the most appropriate, which may cast doubt on the independence of the certification body.

Alternatively, EMBs might directly lead the certification process. They might indicate which certification agency will be in charge of certifying a given product, even though the product might have already received previous certificates. The same strategy could apply to products that have been developed in house or for internal EMB processes.

Who owns the certification? Disclosure agreements

Determining how to validate and confirm the findings of the certifiers is a crucial part of the overall certification process. Either the law or the EMB should establish clear rules regarding how long the certification is valid, the purposes for which it can be used, and the right to access the information or documentation generated by the certification process. Such regulations may result in conflicts of interest between private commercial rights (for example, intellectual property) and democratic needs (for example, citizen oversight of an election process). If the certifier is a third party, a body may be created to review or validate its findings. If stakeholders are allowed to conduct such scrutiny of third-party certifications, they should be required to have a similar skill set as the certifiers.

France: certification reports are only delivered to the EMBs and the vendor itself. Moreover, according to the decisions of the relevant committee (Commission d'accès aux documents administratifs, CADA), the right of access to public information does not apply, because both intellectual property and the electoral process could be endangered. Court rulings have managed to achieve only partial disclosures thus far.

For more details about this case see Annex A.

If vendors choose and contract the certification body, the vendor will usually pay the certification body directly, which may limit the disclosure of the certification reports. However, if the EMB contracts the certification body, there is likely to be more room for a more open disclosure policy, although public administrative rules could be as restrictive as commercial ones. Moreover, EMBs could be subjected to legal constraints imposed by the vendors to protect their intellectual property rights.

Finland: Finland tested Internet voting in three municipalities and an expert review was envisioned, but the proposed non-disclosure agreement (NDA) was not accepted by stakeholders including the Electronic Frontier Finland. They claimed that the NDA included abusive clauses that limited both the right of access to the relevant documentation and the right to publish the final findings.

For more details about this case see Annex A.

How to deal with discrepancies?

Discrepancies are much more significant in an electoral context than in normal certification procedures. ICT election certifications not only aim to guarantee technical performance; they also intend to enhance citizen confidence. Discrepancies may reveal certain information that could be interpreted differently by different stakeholders, depending on their perspective. If experts fail to agree in their findings, election technologies that lack normal oversight by a layperson require a sound communication strategy that enhances overall awareness of the outputs of certification and verification procedures and addresses false expectations.

Discrepancies should be defined early in the process, during the planning stage, in order to avoid any confusion in the execution stage about whether a certain finding by the certifier or a reviewer is considered a discrepancy. Discrepancies may be categorized according to their potential impact on the electoral process—whether they are critical (enough to be 'show stoppers' on election day), major (they may have an adverse effect on the conduct of

elections if compensating controls are not put in place to address them) or minor (they would have no significant effect on election day).

At least three kinds of discrepancies might appear. First, the selection procedure might include some doubtful points regarding adherence to the parameters that have already been set up. For instance, the professionalism of the certification body might be discussed, even within frameworks that enjoy high levels of consensus. The credentials might also cause complaints if there is a margin of appreciation. Second, certification outputs might be controversial if a number of different certification bodies are involved. And finally, the relationship between certification and verification may cause unexpected problems. Although it is normally conceded that the stages covered by an E2E verification do not require previous certifications, it is unclear who is responsible for validating that the system is using E2E tools. Since that statement (which may not be obvious) also needs to be validated (that is to say, certified), discrepancies may easily arise.

Cost considerations

The cost and effort involved in certifying an election technology will vary depending on the quality and quantity of components and documentation involved, which in turn are dictated by the specific requirements of the body contracting the service, whether it is the EMB or the vendor.

The requirements and timeline must be carefully itemized in a request for information (RFI) so that prospective certification service providers can provide detailed cost estimates.

For example, if a source code review is to be included in the service, the RFI must indicate the number of lines of code to be reviewed. If certain dates are prescribed by law, these should be included in the certification requirements. In addition, if specific tests are required, these should be listed with particular parameters that could impact on the cost. The required tests should be described in detail such that both parties would have the same understanding of the kind of tests that are required, and be costed accordingly. Where the certification process will be carried out (at the service provider or EMB/vendor's premises) will also impact on the cost, as will incidental expenses.

It is a good idea to include a checklist of items in the RFI. When responses are received, this makes it easier to decide which items can be removed or added based on cost limitations.

Aside from the actual cost to be incurred for the services of the provider, incidental costs for other related activities should be considered. For example, if a separate group or body will be designated to review, evaluate and validate

the findings of the certification service provider, operational expenses for this body should also be factored in with computation of total cost to be considered.

Norway: A customized open source license enables anybody to access the relevant data for non-commercial purposes. However, the Norwegian case reveals another common drawback in certification procedures conducted by external parties. Due to the difficulties of establishing ongoing pro bono monitoring teams, the Norwegian Government hired external experts to conduct the relevant assessments, despite the apparent contradiction with maintaining an institutional framework based on neutrality and impartiality.

For more details about this case see Annex A.

The cost of certification further varies depending on the organizations involved, their size and the maturity of their processes and procedures. If an EMB decides to implement more than one standard at a time, the number of variables and degree of complexity will increase, and hence raise the costs. Understanding the objectives and benefits of becoming certified will help an organization manage costs and remain compliant with the relevant standards.

Once a system is certified it will be subject to updates and continual improvement. This requires regular reviews and audits, and represents an additional cost to certification

Time

For certifications to be relevant, the certification process must satisfy the following time-based requirements:

1. *Certification must be completed pursuant to the legally prescribed time frame*. Certain jurisdictions have strict legal requirements regarding when the certification process should be implemented and the results released.
2. *Certification reports must be timely—not too early, never late*. Decision-makers and EMBs must be informed in a timely manner of the results of certifications to ensure that they are able to implement corrective measures (if needed) in time for elections.
3. *The certifier must be able to complete the requirements within a specified period*. Unlike regular audit reports, the law (if not the constitution) prescribes the election period. More often than not, the election date cannot be, and is not, postponed. Since many governmental budgetary systems rely on multiple layers of bureaucracy, and procurement processes are restricted, election technology is usually finalized and

purchased later than would be ideal. Therefore the certifying body must be able to satisfactorily review the technology within a short, non-extendable time frame.

4. *Certification must be regularly reviewed and/or refreshed to ensure that the different systems used are still effective*. Given that certification helps project a fair and credible system, it is useful to re-certify for every election even if doing so is not legally mandated.

Philippines: The Philippine Automation Law requires the domestic Technical Evaluation Committee to certify the automated elections system, including its hardware and software components, no later than three months before an election.

For more details about this case see Annex A.

Transparency and communication

Many countries require elections to be transparent, which includes giving all electoral stakeholders access to documentation and other relevant aspects of the electoral process. In some countries, citizens have the opportunity to check all parts of the electoral process, including observing the counting process.

Germany: The Supreme Court decided in 2009 that the electoral law at that time did not live up to the requirement of transparency, and banned voting devices that were in use. The court highlighted that real transparency is not only formal openness; it also involves citizens' ability to understand the key stages of an election process without specialized knowledge.

For more details about this case see Annex A.

The election technology certification process and outputs can increase the transparency of an election among stakeholders, election officials, polling workers, voters and election observers. EMBs can use the outputs from different stages of the certification process to convince stakeholders that all necessary steps were taken to guarantee an election of the highest standard. The outputs may even be used as evidence in court disputes.

Hurdles to transparency

Not all EMBs make the most of these outputs in terms of transparency and trust generation, and some choose to keep the outputs confidential. The following are concerns typically raised in that regard.

NDAs demanded by vendors or certification bodies. Some may argue that vendor-associated proprietary intellectual property of certain hardware and software products should be protected and not be easily available to the general public. Some may also argue that the source code of various software components should only be made available to third parties subject to the signing of a carefully worded NDA.

Technical information can be misunderstood, and *some stakeholders can intentionally misinterpret very detailed information*. This is a valid concern that can be addressed by a clarifying response from the EMB and possibly also the vendor. The response should describe remedial actions and correct any misrepresentations.

The release of too many details creates new vulnerabilities and undermines the system's integrity. This a common concern, which is not valid. Any attacker who is interested in exploiting the weaknesses and vulnerabilities of an election technology should be assumed to know these details already.

Kazakhstan: The Sailau electronic voting system was first used in 2004, and it was discontinued in 2011. While voting machines were subject to external review, the requirements for certification and the final report were not made available to the public.

For more details about this case see Annex A.

Improving transparency through the outputs generated during the preparatory stages of the certification process

Prior to contracting evaluators, reviewers or consolidators, the EMB may publish the following information:

- *Election settings*: The EMB may release information gathered throughout the feasibility analysis, including scheduling constraints, legal and technical requirements of the overall technology, as well as available financial resources.
- *Details about component evaluation*: The EMB may publish details about the process of determining the technical requirements. It may also publish information about the evaluation method, including the requirements of the evaluation.
- *Evaluation service procurement requirements and results*: This may include publishing the terms of reference, including the identities of interested parties, the results of the procurement process and costs. Many procurement processes are public in nature.

Transparency through the outputs generated during the evaluation and review phase of the certification process

The EMB may, as part of its quality control process, involve public or accredited groups such as political parties, civil society or academic researchers and other experts to review the evaluation reports of different components. Their reports can be made public prior to consolidating the various other documents.

Evaluation reports: During the early stages of the evaluation process, and prior to implementing corrective measures, the EMB may release initial evaluation reports. It may decide to discuss corrective measures with the end user, and may release strategic information revealing which corrective measures have been taken, and eventually publish the final evaluation report.

Reviews: As a further transparency measure, the EMB may decide to publish the results of independent reviews.

Belgium: The College of Experts conducts an independent review/evaluation. Additional certification is provided through a private certification company accredited by the Belgian Government. The college must report its findings to parliament and the Ministry of Interior, and these reports are generally published thereafter. No details about the certification by the private company are available to external stakeholders.

For more details about this case see Annex A.

Improving transparency with the final report

The EMB's response to the results of the certification review should include the following information, regardless of whether it is released to selected stakeholders or the general public. Since stakeholders have different interests in the election technology, the reports may be released with different target audiences in mind, such as political parties, non-governmental organizations and electoral observers (both domestic and international). This response might include both general and specific information about the certification process.

If the election technology was certified, the EMB should explain precisely what requirements the system was shown to fulfil. It may also increase transparency about other aspects of the election preparation process to help build public trust in and acceptance of election technologies. Specific information an EMB may want to share might include the selection criteria and credentials of the evaluation body and reviewers; requirements against which the evaluation was conducted; comments about the evaluation reports; certificates; and the EMB's interpretation and conclusions.

In addition to releasing different documents and information generated throughout the certification process, there are complementary methods of ensuring transparency. For example, allowing public review without major restrictions helps stakeholders increase their trust in the election technology.

Philippines: Pursuant to the Philippine Automation Law, the Philippine EMB allowed accredited parties (including critics and stakeholders) to review the source code to be used for the 2016 elections months before the actual polls, alongside the official certification evaluation.

For more details about this case see Annex A.

Another approach to encouraging transparency is for an EMB to launch an education campaign explaining the different technologies being subjected to certification. This increases public awareness of both the certification process and the technology.

Brazil: The EMB organized public tests of the electronic voting system, during which it invited computer scientists and interested parties to attempt to find external vulnerabilities in the system.

For more details about this case see Annex A.

Venezuela: No certification was deemed necessary, but a source code review process was made accessible to interested stakeholders.

For more details about this case see Annex A.

Summary

The final consolidation report of the certification process should arguably be made available to the general public. However, there is also convincing evidence that it is beneficial to publish intermediate outputs during each major phase of the certification process. Releasing information and documents to the general public might increase credibility and public acceptance of the entire election process, as long as the system essentially implements the proposed requirements. Yet if major flaws and shortcomings are detected in the system, this might significantly damage the EMB's reputation. While publishing information and documents throughout the quality assurance process requires an EMB to allocate further resources to communicate with the general public, doing so will benefit public education and contribute to

informed discussion. The EMB may also consider that electoral disputes arising during the quality assurance process might need to be taken into account and mitigated before the election. Transparency-enhancing measures are closely related to the means of communication in place: communicating the separation of duties (k-resilience) that prevent single points of failure might be one means of ensuring the transparency of the entire election process (see Annex B).

Conclusions

This Guide has discussed how the certification of election technologies has been approached differently around the world. It offers arguments both in favour of and against certification, and introduces the Quality Assurance Framework to provide guidance to electoral stakeholders during third-party assessments of election technologies. This framework covers planning, time and cost considerations, and the communication of results.

On the basis of this Guide, it can be concluded that:

1. *Certification can enhance citizen confidence and election integrity*. The Quality Assurance Framework helps EMBs plan for the certification of election technologies, including measures necessary to achieve transparency, international recognition and local acceptance.
2. *Certification is complex*. The Quality Assurance Framework simplifies planning and conducting certification processes.
3. *Certification of election technologies is time critical*. The Quality Assurance Framework helps EMBs integrate certification activities into their overall project plan.
4. *Certification requires prioritization due to resource limitations*. The Quality Assurance Framework provides EMBs with guidance on how to prioritize certification tasks based on their importance.
5. *Certification of election technology is a continuing process*. The Quality Assurance Framework requires ongoing evaluation and improvement, and supports third-party oversight and external review.
6. *Certification and election observation are complementary*. Certification can support (but not replace) electoral observation. Conversely, electoral observation cannot be seen as a certification measure.

7. *Certification may expose weaknesses*. When third-party evaluations identify weaknesses, EMBs need to take measures to minimize the risks to their trust and credibility.
8. *Certification needs to be properly communicated*. All certification processes should include a communication strategy and an acknowledgment of what certification can achieve (as well as its limitations).
9. *Certification content and evaluator selection are equally essential*. Providing third-party evaluators with clear requirements is as crucial for a successful certification as their independence and qualifications.
10. *Certification needs a context-specific approach*. Sociopolitical factors and national legislation are important guiding principles for drafting requirements for certification.

Annex A: Case Studies

Australia

New South Wales

The New South Wales Election Commission (NSWEC) procured iVote, an online voting system for the 2015 State Elections. The NSWEC does not believe that the current maturity of the remote internet voting system market is sufficiently advanced to allow effective certification by any organisation. It also sees it it as problematic to devise and apply standards when the actual requirements for systems are not common across jurisdictions. The NSWEC is of a view that each jurisdiction has a different social and political mix and different drivers for implementing these systems, hence the concept of standard creation will be difficult. Moreover, the standardisation process should not focus on the technology components of the system but rather its operation and outcomes. The standards which the NSWEC envisages would be most effective are those that demonstrate that the system meets or exceeds the integrity of current electoral processes and satisfies stakeholder expectations. The NSWEC does not believe a standard specific to electronic voting is necessary, but rather one which is more akin to quality standards such as ISO 9000.

The NSWEC is interested in improving effective transparency for its systems but does not believe that necessarily means providing unfettered public access to system documentation. The NSWEC is mindful of the overheads of increased transparency regimes and believes the public interest is best served when the effort to provide transparency is balanced against the added confidence these activities give to the electorate.

Victoria

The state of Victoria in Australia developed an E2E verifiable kiosk-based voting system called vVote from 2011 to 2014. vVote was designed and implemented by a team from the University of Luxembourg, the University of Surrey and Crypto Workshop, plus a group of programmers working for the Victorian Electoral Commission (VEC).

The project was launched in 2011, requirements were committed in December 2012 and the software development process ended in December 2013. The developer teams reviewed each other's code to ensure internal quality control. Late in 2013, a tender for a third-party reviewer was organized. In March 2014 a third-party evaluator, the DemTech Group, evaluated the entire system and produced a report that was published on the VEC's homepage, accompanied by a detailed response from the VEC. No certification was sought by the VEC. All documents are available from the commission.

The vVote system was piloted during the 2014 Victorian state election, when it was open to three groups of voters: those with disabilities, those who could not understand English, and residents abroad in London. It collected 1,121 votes.

Key features

- A kiosk-based voting system was piloted in 2014; for selected voter groups only.
- The pilot system was designed and implemented by the academia with the EMB.
- Peer review was conducted for the pilot system.
- Third-party evaluation was organized after the pilot, and the report was made public on the EMB website.

Reference

Victorian Electoral Commission, <http://www.vec.vic.gov.au/Voting/ElectronicVotingDetail.html>, accessed 16 October 2015

Austria

In Austria, a test case for Internet voting was conducted in the area of student elections. Austrian student elections are special, as they are regulated by federal law and have a high legal value. As part of the Internet voting euphoria at the beginning of the millennium, the Austrian Parliament changed the relevant law to allow Internet voting as long as two conditions were met: (1) identification was done using smart cards with digital signatures and (2) the software was certified by the certification authority for digital

signatures, A-SIT. In the regulations accompanying the law, the requirements for the certification were set by CoE Recommendation Rec(2004)11 and relevant protection profiles.

Austria's first (and, to date, only) use of Internet voting was conducted in 2009. The certification process was to be concluded at least 60 days before election day. This deadline was kept, but A-SIT defined five operational conditions that were to be fulfilled during the vote for the certificate to be valid. This essentially meant that A-SIT had to monitor the implementation of the election. In addition, it had to re-certify minor changes to the software, for which an additional certificate was issued. The final report of the evaluation was only made accessible to representatives of the political parties during a limited public event, which led to a lot of public criticism.

Key features

- Internet voting technology was mandated to use CoE Recommendation Rec(2004)11 and relevant protection profiles after certification of a test case by the certification authority for digital signatures.
- Certification was to be concluded at least 60 days before election day.
- The costs for the evaluation process were paid by the oversight body, the Federal Ministry of Science and Research.
- Only the certificate(s) were publicly accessible.
- The final evaluation report was only available to a limited audience.
- The certification authority was assigned by law and is independent and competent.

Reference

Krimmer, Robert and Ehringfeld, Andreas and Traxl, Markus, *E-Voting bei den Hochschülerinnen- und Hochschülerschaftswahlen 2009. Evaluierungsbericht* (Vienna: Austrian Federal Ministry of Science and Research, 2010), <http://www.e-voting.cc/wp-content/uploads/downloads/2015/04/Evaluierung_OeH-Wahl_E-Voting.pdf>, accessed 15 November 2015

Belgium

The Belgian E-voting Act was approved in 1994 and two voting systems were deployed, covering up to 44 per cent of the electorate. In 2012, one of these systems was replaced by a new platform adapted to contemporary requirements.

An independent review/evaluation was conducted by the College of Experts, and additional certification was provided by a private certification company accredited by the Belgian Government. The College of Experts is an expert

committee appointed by parliament that evaluates the country's electronic voting technologies. The college begins reviewing the automated voting systems 40 days before elections. Members are entitled to request any information from technology vendors, including source codes and copies of software. They may also visit polling stations, copy software in use on election day and conduct other activities. The college must report its findings to parliament and the Ministry of Interior within 15 days after elections, and reports are generally published thereafter.

In addition, each political party that has at least two members of parliament may designate an IT expert to receive the source code of the e-voting systems and examine it. While they must keep the source code confidential, it is published after the election.

In 2007, federal and regional administrations commissioned a consortium of seven Belgian universities to conduct an independent comparative study of e-voting systems—known as the BeVoting study—to propose which one best fit international standards and the Belgian electoral legislation. The proposal included the requirements for the new voting system in such detail that the report may serve as a technical appendix to the call for tenders. The CoE also evaluated the compliance of the BeVoting Study with its Recommendation Rec(2004)11.

Key features

- Requirements were only indirectly derived from legislation: they were defined as finding an existing solution that best matches the legislative framework.
- Evaluation and certification were conducted independently of each other.
- Reports by the College of Experts are publicly accessible.
- No details about the certification by the private company are available to external stakeholders.

References

BeVoting Reports [Part I (comparison and evaluation), Part II (proposals) and CoE's Report], <http://www.elections.fgov.be/fileadmin/user_upload/Elections/fr/presentation/bevoting-1_gb.pdf>, <http://www.elections.fgov.be/fileadmin/user_upload/Elections/fr/presentation/bevoting-2_gb.pdf>, accessed August 2015, <http://www.elections.fgov.be/fileadmin/user_upload/Elections/fr/presentation/Compliance_Belgian_BeVoting_Rec_1_0_final_18_02_08.pdf>, accessed August 2015

PourEva, 'Expert Reports', <http://www.poureva.be/spip.php?rubrique19>, accessed 16 October 2015

Organization for Security and Co-operation in Europe Office for Democratic Institutions and Human Rights, 'Elections in Belgium', <http://www.osce.org/odihr/elections/belgium>, accessed 16 October 2015

Vegas González, Carlos, 'The New Belgian E-voting System', *Electronic Voting 2012* (Bonn: GesellschaftfürInformatik, 2012), pp. 199–211, <http://www.e-voting.cc/wp-content/uploads/downloads/2012/07/199-211_Vegas_Belgian-E-voting.pdf>, accessed 16 October 2015

Brazil

Brazil's EMB, the Tribunal Superior Eleitoral (TSE), developed electronic voting machines that were introduced in 1996 and deployed nationwide shortly afterwards. The machines' apparent simplicity was designed to facilitate the transition from a paper-based to a computerized system.

The TSE has final authority over the system's source code, which has not been certified by an outside authority. The legal framework requires the TSE to make the final source code available to political parties and the Bar Association (Ordem dos Advogados do Brasil, OAB) 120 days before an election. After 2000, in the wake of heightened scrutiny of the system, the TSE began to allow outside actors to review the source code, but only a few political parties regularly participated in these reviews, and obtained the required expertise from affiliated academics or contracted companies.

The first comprehensive, independent and non-partisan audit of code and equipment was conducted several years after the adoption of electronic voting in 2001 and 2002 by eight computer scientists at the State University of Campina. Since then, the TSE has sponsored a few additional independent audits of the code, generally by university researchers.

The OAB hired an outside company to examine the source codes in 2004. Since then only minimal auditing has been conducted due to the high costs and a lack of internal capacity. In 2009 and 2012, the TSE organized public tests of the system and invited computer scientists and interested parties to attempt to find external vulnerabilities in the electronic voting system. The first test did not provide access to source code, while the second one did.

Key features

- Brazil is a large country that uses a single e-voting solution nationwide.
- The voting machines were developed by the EMB, which owns the source code.
- No formal evaluation or certification process was conducted by the EMB.
- The EMB has opened the review to public tests.

- Some stakeholders were granted access to technical details and could conduct assessments at their own expense.
- Assessments were conducted by the OAB as well as political parties that in turn relied on academics and contracted companies.
- The high costs for stakeholders limit the extent to which stakeholders can conduct assessments themselves.

References

National Democratic Institute [NDI] and International Federation for Electoral Systems [IFES], *Implementing and Overseeing Electronic Voting and Counting Technologies* (Washington, DC: NDI and IFES, 2013), <https://www.ndi.org/files/Implementing_and_Overseeing_Electronic_Voting_and_Counting_Technologies.pdf>, accessed 16 October 2015

van de Graaf, Jeroen and Felipe, Ricardo, 'Uma Analise da Seguranca da Urna Electronica Brasileira', Dissertation, Universidade Federal de Santa Catarina, 2003, <https://repositorio.ufsc.br/bitstream/handle/123456789/85004/198467.pdf?sequence=1>, accessed 16 October 2015

Estonia

Estonia is the only country in the world that provides its citizens in all elections with an optional Internet voting channel. A major technical cornerstone is the use of digital signatures to identify voters and the use of a hardware security module to decrypt the Internet votes for counting.

Neither the law nor the EMB has prescribed the formal external evaluation and certification of the system. However, the EMB contracts undisclosed experts to provide an opinion on the software but does not disclose the requirements, the reports or their authors.

In addition, for each election the EMB hires an audit company to oversee the conduct of Internet voting. It checks the conduct against a published operation manual. The completeness of the manual is not checked, nor are there any deviations from it. The reports are not made public.

Key features

- Expert opinions are given about the source code before the election, and a review of the operations is conducted.
- The opinion is conducted before the election and the review of operations is conducted during the election.
- The costs of the reviews are paid directly by the EMB.

- No reports are made public.
- The EMB developed the requirements (operations manual) for the review of operations.

References

Springall, Drew, et al., 'Security Analysis of the Estonian Internet Voting System', *Proceedings of the 21st ACM Conference on Computer and Communications Security* (Scottsdale: ACM, 2014), <https://jhalderm.com/pub/papers/ivoting-ccs14.pdf>, accessed 16 October 2015

Organization for Security and Co-operation in Europe/Office for Democratic Institutions and Human Rights, 'Elections in Estonia', <http://www.osce.org/odihr/elections/estonia>, accessed 16 October 2015

Finland

Finland piloted Internet voting from supervised contexts in 2008. It was a limited project that only covered three municipalities—Karkkila, Kauniainen and Vihti—during one election. Usability drawbacks were discovered that justified the withdrawal of the Internet voting channel.

The Finnish EMB decided to submit the project to external review by an academic group, but other stakeholders (for example, Electronic Frontier Finland and a computer expert) refused to accept the non-disclosure agreement (NDA) proposed by the vendors, and did not participate in the review process.

Key features

- This was a limited project that used Internet voting from supervised contexts.
- Usability failures led to a Supreme Court ruling that banned this voting channel.
- A controversial NDA was used for external evaluations.

References

Aaltonen, Jussi, 'Electronic Voting Case Law in Finland', in Ardita Driza Maurer and Jordi Barrat (eds.), *E-Voting Case Law: A Comparative Analysis* (Farnham: Ashgate, 2015), pp. 173–81

Barrat, Jordi, 'El voto electrónico ante intereses contradictorios: la razón comercial contra el principio democrático. A propósito de los compromisos comerciales de confidencialidad (CCC)', *Democracia digital, participación y voto electrónico* (Valencia: CEPS, 2010), pp. 57–69

Vähä-Sipilä, Antti, *A Report on the Finnish E-Voting Pilot* (Helsinki: Electronic Frontier Finland, 2009), <http://www.effi.org/system/files?file=FinnishEVotingCoEComparison_Effi_20080801.pdf>, accessed 20 August 2015

Whitmore, Keith, *Information Report on the Electronic Voting in the Finnish Municipal Elections Observed on 26 October 2008* (Strasbourg: Congress of Local and Regional Authorities, 2008)

France

France uses voting machines as well as Internet voting. Voting machines are used by a limited number of municipalities that have to be approved in advance by the Ministry of Internal Affairs, while French citizens living abroad can use Internet voting to select up to 11 MPs in the Lower Chamber.

Voting machines are approved by the Ministry of Internal Affairs based on a certificate issued by a qualified agency. These entities must comply with Annex A of regulation EN45004 or an equivalent regulation, and should be validated by the French Accreditation Committee (*Comité Français d'Accréditation*) or a similar entity within the European Cooperation for Accreditation framework.[2]

Different suppliers may request to have their voting machines approved, and each municipality chooses which vendor will deploy voting machines in each local jurisdiction. Municipalities buy the voting machines and take care of them. The certification process only covers the machines and the suppliers' internal management procedures, including the information they give to the local authorities. It does not cover the security and management standards used by local authorities. The vendors are required to provide general guidelines to their clients, but the implementation depends largely on the local authorities.

Certification reports are not public. Vendors select and pay a certification agency, and the reports are only delivered to the EMB and the vendor. Moreover, according to a 26 January 2006 recommendation by the *Commission d'accès aux documents administratifs*, an official consultative board, the certification reports can be withheld from the public on the grounds that industrial secrecy and the proper implementation of the elections could be compromised. During the 2007 presidential elections, court decisions managed to partially disclose certification reports.

Internet voting follows a different strategy. Audits are carried out by a computer professional specialized in security, who has no financial interest

[2] 'Art. 2.1, Arrêté du 17 Novembre 2003 portant approbation du règlement technique fixant les conditions d'agrément des machines à voter', <http://www.interieur.gouv.fr/content/download/1775/18612/file/reglement_technique_machine_voter.pdf>, accessed 20 August 2015

in the company that produces the voting system, who has experience in the analysis of voting systems and who participated in a workshop for experts on electronic voting organized by the *Commission nationale de l'informatique et des libertés* (Paragraph II of article R. 176-3 of the Electoral Code). The audit verifies the respect for secrecy, and the reliability and accessibility of the vote. It covers the full breadth of the system to be used and the operations to be carried out prior to the vote, the use of the voting system during the elections, the tally and the storage of data after the vote (Article 2/Arrêté 27 April 2012).

Subsequent reports have not been published. OSCE/ODIHR (2012:11) suggested in 2012 that 'the internet voting security requirements, as well as the methodology and results of security assessments, audit protocols, results of all audits performed, the analysed source code, and minutes of all proceedings be made available to the general public to enhance confidence in the internet voting process'.

Key features

- Two types of election technologies are used: voting machines and Internet voting, with different methods of certification:
  - For voting machines, certification is performed by a qualified third party selected by the vendors, which pay for the certification services. The voting machines are approved by the EMB after the certification.
  - For Internet voting, an audit is done by a computer security professional who meets specific requirements.
- There is limited disclosure of certification reports for voting machines, since these are only delivered to the electoral authorities and to the vendor.
- Partial disclosure is allowed due to court rulings.
- Reports are not published for either technology.

References

Barrat, Jordi, 'The French Conseil Constitutionnel and Electronic Voting', in Ardita Driza Maurer and Jordi Barrat (eds.), *E-Voting Case Law: A Comparative Analysis* (Farnham: Ashgate, 2015)

Barrat, Jordi, 'The Certification of E-Voting Mechanisms: Fighting Against Opacity', in Robert Krimmer and Rüdiger Grimm (eds.), *Electronic Voting 2008* (Bonn: Gesellschaft für Informatik, 2008), pp. 197–206

Gugliemi, Gilles and Ihl, Olivier (eds.), *Le vote électronique* [The Electronic Vote] (Paris: LGDJ, 2015)

Ordinateurs de vote, <http://www.ordinateurs-de-vote.org>, accessed 16 October 2015

Organization for Security and Co-operation in Europe/Office for Democratic Intuitions and Human Rights, 'Elections in France', <http://www.osce.org/odihr/elections/france>, accessed 16 October 2015

Germany

In Germany, electronic voting machines were used in parts of the country, and they did not provide for a VVPAT. They were evaluated and certified by the Physikalisch-Technische Bundesanstalt in Berlin, and only the certificate was made public. The evaluation reports remained closed. This was the case until in 2009 when the Supreme Court decided—upon an appeal from a citizen—that voting machines without a VVPAT should not be used, as they do not allow layperson citizens to completely understand the voting and counting process, or the ability to see if there have been any manipulations.

Key features

- In Germany, a single type of voting machine was used in parts of the country for federal elections. The machine did not provide a VVPAT.
- A single accreditation body was established by law, which evaluated and certified the system according to the legal requirements.
- The evaluation report was not made public.

Reference

Bundesverfassungsgericht, Decision from 3 March 2009, <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2009/03/cs20090303_2bvc000307en.html>, accessed October 2015

India

After initial pilots were completed with EVMs in the late 1970s and early 1980s, a parliamentary act introduced e-voting in 1988; nationwide deployment was achieved in 2004. The inclusion of paper trail audits has been subject to different lawsuits, ending with a Supreme Court ruling in October 2013 that requires them. VVPAT machines were introduced during Loksabha elections-2014 as a pilot in a few states.

The Indian voting machines were devised and designed by an independent technical expert committee consisting of a group of professors in computer science. The EVMs are manufactured in collaboration with two public sector enterprises after a series of meetings, test-checking of the prototypes by the technical expert committee and extensive field trials. The voting machines

are now produced by these two companies, under the supervision of the independent technical expert committee.

While testing does play a role in the work of the EMB, it is done by the independent technical expert committee constituted by EMB. Due to increased concerns expressed by election stakeholders during the 2009 elections, the EMB invited critics to share specific information about perceived or actual vulnerabilities in the EVM system. The EMB additionally puts emphasis on several security procedures and rituals to prove the accuracy, efficacy and neutrality of the system.

For the 2009 and 2014 parliamentary elections, the usage of the EVMs went smoothly. However, the Election Commission of India (ECI) has always been interested in independent testing and exploring innovations for future elections.

Key features

- Voting machines were devised and designed by an independent technical expert committee and manufactured by two public sector companies.
- Tests and checks of the prototypes were conducted by the technical expert committee.
- Extensive field trials are conducted.
- Production of the voting machines under supervision of the technical expert committee.

References

Election Commission of India, 'FAQs – Electronic Voting Machines', <http://eci.nic.in/eci_main1/evm.aspx>

Philipps, Mark and Soudriette, Richard, 'Testing Democracy: How Independent Testing of E-Voting Systems Safeguards Electoral Integrity', *Electronic Voting 2012* (Bonn: Gesellschaft für Informatik, 2012), <http://www.e-voting.cc/wp-content/uploads/downloads/2012/07/159-170_Soudriette-Phillips_Testing-Democracy.pdf>, accessed 16 October 2015

Prasad, Hari K. et al., 'Security Analysis of India's Electronic Voting Machines', *17th ACM Conference on Computer and Communications Security* (Chicago: ACM, 2009), <https://indiaevm.org/evm_tr2010-jul29.pdf>, accessed 20 September 2015

Kazakhstan

The Sailau electronic voting system was first used in 2004, and was discontinued in 2011. The system was deployed in supervised contexts and

consisted of a direct recording electronic machine, which used two devices to retrieve and process voting data. Poll books were also integrated into the system.

Voting machines were subject to external review. However, the requirements for the certification (and the final report) were not made available to the public.

Key features

- Voting machines were used from 2004 and discontinued in 2011.
- The requirements for certification and the certification reports were not published.

References

Jones, Douglas, 'Kazakhstan: The Sailau E-Voting System' in Michael Yard (ed.), *Direct Democracy: Progress and Pitfalls of Election Technology* (Washington, DC: International Foundation for of Electoral Systems, 2010), <http://homepage.cs.uiowa.edu/~jones/voting/IFESkazakhstan.pdf>, accessed 20 September 2015

Organization for Security and Co-operation in Europe Office for Democratic Institutions and Human Rights, 'Elections in Kazakhstan', <http://www.osce.org/odihr/elections/kazakhstan>, accessed 16 October 2015

Netherlands

The EMB (Kiesraad) contracted a private company to develop software for nomination of parties and candidates, and to tabulate results and allocate seats. An EMB expert group developed a detailed technical specification based on the applicable legal framework for this purpose in June 2009. This specification was subsequently updated for newer versions of the software, most recently in January 2014.

At the request of the EMB, third-party companies were contracted to assess the result tabulation and seat allocation software in regards to the following two aspects:

- the degree to which the software meets the established specification for calculating the result and distributing the seats; and
- the extent to which the software meets the requirements of the electoral act.

A first assessment was conducted in February 2011 for the general elections in September 2011; a second assessment was done in February 2015 for the senate elections at the end of May 2015. The EMB also requested academic

legal experts from the University of Utrecht to assess the legal correctness of the technical specification.

The EMB takes a highly transparent approach and publishes all requirements, assessment reports and system source code on its website.

Key features

- The national EMB provides a software solution.
- The adoption of a system is based on a decision of local election administrative bodies.
- The EMB defined technical requirements through an expert group.
- The software was independently assessed against the technical requirements.
- The technical requirements were independently assessed against the legal framework.
- Assessments were completed approximately one year after the requirements were defined and at least three months before election day.

Reference

Ondersteunende Software Verkiezingen, <http://kiesraad.nl/artikel/ondersteunende-software-verkiezingen-osv>, accessed 16 October 2015

Norway

The Norwegian Internet voting project was used in 2011 (for local elections) and 2013. It was later stopped due to political reasons. No certification was deemed necessary, as the Internet voting procedures were claimed to comply with E2E verification. Both supervisions, in conjunction with the disclosure of all relevant data concerning Internet voting devices, were deemed to provide the same (or higher) degree of confidence as certification. However, E2E mechanisms still rely on tasks that can only be conducted by IT experts. Therefore, this solution may ease the controls over the voting application and allow any interested expert to carry out his/her own verification, but—in contrast to what happens with traditional paper-based elections—average citizens will still remain excluded and the system is based on proxy trust.

Moreover, E2E verification assumes that an external third party with no conflicts of interest will carry out the relevant tasks, but (as the Norwegian example shows), that might not happen and the E2E framework may never be implemented. Hiring external experts, as the EMB did, somehow contradicts E2E's rationale.

The Internet voting system implemented in Norway included an auditor module for monitoring transactions within the system. It also employed several organizations to provide system and security audits. In addition, the ministry contracted an independent auditor to check that key stages of the vote authentication and counting processes were conducted accurately, and that recorded votes were not changed during the cleansing, mixing and tallying stages of the process. External evaluation studies were also contracted by the EMB, which were designed to cover social and legal issues.

Key features

- Internet voting procedures were claimed to comply with E2E standards.
- No certification process was in place.
- Customized open source licenses enable anybody to access the relevant data for non-commercial purposes, including review.
- Despite openness, it was difficult to gather experts to conduct pro bono reviews.
- Due to a lack of experts to conduct open reviews, external auditors were contracted by the ministry to monitor strategic issues from both IT and socio-legal perspectives.

References

Government of Norway, 'Evaluation Reports 2011', <https://www.regjeringen.no/no/dokumenter/evaluering-avforsoket-med-e-valg-2011/id684923/>, accessed 16 October 2015

Government of Norway, 'Evaluation Reports 2013', <https://www.regjeringen.no/no/dokumenter/Internettvalg/id764303/>, accessed 16 October 2015

Organization for Security and Co-operation in Europe/Office for Democratic Institutions and Human Rights, 'Elections in Norway', <http://www.osce.org/odihr/elections/norway>, accessed 16 October 2015

Stenerud, Ida Sofie Gebhardt and Bull, Christian, 'When Reality Comes Knocking Norwegian Experiences with Verifiable Electronic Voting', in *Electronic Voting 2012* (Bonn: Gesellschaft für Informatik, 2012)

Philippines

For the 2010 presidential and local elections, the Philippines, with approximately 50 million local voters and a sizable number scattered around the world, implemented an automated election system (AES). The AES covered key aspects of the Philippine electoral process, including preparation of election data for the configuration of the ballots, casting of votes on machine-readable ballots, receiving and counting of votes using electronic

voting machines, electronic tabulation using electronic results, and electronic transmission of results to the relevant canvassing levels.

The Automation Law required that an independent body certify the AES. It specifically stated that a Technical Evaluation Committee (TEC) composed of members of the Department of Science and Technology, the Commission on Information and Communications Technology and the Commission on Elections (COMELEC) should be formed. Using identified document results, and with the support of an international certification entity (ICE), the TEC's primary task was to certify that the system (including its hardware and software components) was operating properly, securely, accurately and in accordance with the law. They were to do so no later than three months before the election.

Another independent body called the Advisory Council was tasked to recommend a short-list of established ICEs to support the TEC's certification. The members of the Advisory Council were legally required to be of 'known independence, competence, and probity' and to come from different sectors of the country, including the government sector (ICT, science and technology and education ministries) and the private and non-governmental sector (ICT professional organizations, non-governmental electoral reform organizations).

After undergoing government procurement procedures, the Philippine EMB contracted an international entity to review the AES. In turn, this international entity used the certification test reports summary to audit the system's accuracy, functionality and security controls. After the international entity's review—and based on the requirements and guidelines for AES certification embodied in the Philippine Automation Law—the TEC issued the corresponding certification. The TEC stated that, in accordance with the Automation Law, the AES could, with full adoption of the recommended compensating controls, be used securely, accurately and properly by voters, boards of election inspectors, local and national boards of canvassers, and COMELEC in the 10 May 2010 national and local elections. The source code was also held securely at the Philippine Central Bank in accordance with the Automation Law.

Thus the 2010 elections were held using a certified automated system. In accordance with the Automation Law, a random manual audit with the Parish Pastoral Council for Responsible Voting, an accredited citizens' arm, was conducted.

Key features

- The EMB was the sole customer purchasing a single solution for nationwide use.
- The EMB paid for the AES certification.
- The general requirements and guidelines for AES certification were embodied in the Automation Law.
- The AES certification was issued by an independent committee and not by the EMB.

References

Republic of the Philippines Commission on Elections, TEC Resolution No. 2013-001, <http://www.comelec.gov.ph/?r=Archives/RegularElections/2013NLE/Resolutions/tecres2013001>, accessed 16 October 2015

Republic of the Philippines Commission on Elections, Republic Act No. 9369, <http://www.comelec.gov.ph/?r=References/RelatedLaws/ElectionLaws/AutomatedElection/RA9369>, accessed 16 October 2015

Switzerland

Each canton using electronic voting needs to get approval from the Federal Chancellery for it to be introduced, as well as after the expiry of initial approval, any 'significant' changes in the system, geographical expansion or an expanded electorate.

The specification of confederation-wide requirements is defined in 'Anforderungskatalog für eidgenössische Volksabstimmungen mit der elektronischen Stimmabgabe'. Systems need to comply with domestic (federal and cantonal) legislation and relevant international legal obligations—the European Convention on Human Rights and International Covenant on Civil and Political Rights and CoE Recommendation Rec(2004)11.

Federal Chancellery approval is based on tests monitored by the chancellery as well as the provision of detailed documentation. Approval starts six to nine months before the election at the latest.

Beyond this approval, there are certification requirements as follows:

- for usage by more than 30 per cent of the electorate, valid certification and audit reports need to be provided for individual verifiability;
- for usage by more than 50 per cent of the electorate, complete (individual plus universal) verifiability is required;
- to date, all uses have involved less than 30 per cent of the electorate.

Key features

- Cantons decide on the usage of voting technology, which requires approval by federal authorities.
- The need for certification depends on the percentage of the electorate that may use the system.

References

Federal Chancellery, *New Provisions for Online Voting. Test Conditions* (Bern: Federal Chancellery/Swiss Conferedation, 2015), <https://www.bk.admin.ch/themen/pore/evoting/07979/index.html?lang=en>, accessed 15 October 2015

Kuoni, Beat, 'E-Voting Case Law: A Swiss Perspective', in Ardita Driza Maurer and Jordi Barrat (eds.), *E-Voting Case Law: A Comparative Analysis* (Farnham: Ashgate, 2015)

Organization for Security and Co-operation in Europe/Office for Democratic Institutions and Human Rights, 'Elections in Switzerland', <http://www.osce.org/odihr/elections/switzerland>, accessed 15 October 2015

USA

The United States Election Assistance Commission (EAC) created voluntary voting system guidelines (VVSG), which specify the minimum standards applicable to electronic voting. The EAC has developed a comprehensive program by testing all voting systems against these guidelines. The EAC does not evaluate electronic voting and counting equipment systems itself, but accredits testing labs (voting system test laboratories or VSTLs) that evaluate voting systems, voting devices and software against the VVSG to determine whether they provide all of the required functionality, accessibility, and security capabilities. After completing the evaluation phase, the VSTLs provide a set of recommendations to the EAC, which upon review of the Commission's executive director determines whether to issue a certification. Once an e-voting solution is certified, a system is allowed to bear an EAC certificate sticker and can be advertised as having obtained EAC certification.

While the VVSG certification process can be an effective method of ensuring the integrity of the e-voting or counting system, electoral bodies must consider that the certification process (depending on the number of issues discovered) may take approximately 12 months The examination process to certify e-voting or counting systems can also be expensive. VVSG certification guidelines are designed to comply with US laws, and some aspects of the certification process may not be directly applicable to other countries. These challenges must be carefully evaluated and balanced with the benefits of following such a certification approach.

Key features

- A large market with several competing vendors and many local electoral administrations that can choose which technology to utilize.
- Domestically developed and maintained federal standards.
- A certification process including evaluation in testing laboratories and certification by the federal EMB.
- VVSG establishment of clear technical requirements for vendors.
- Certification allows vendors to market their solutions to different electoral administrations.
- States can regulate whether and how to utilize certification and require either:
  - no evaluation or certification at all;
  - evaluation against federal standards;
  - evaluation against federal standards by an accredited laboratory; or
  - evaluation against federal standards by an accredited laboratory and certification by a federal agency.
- Requirements, evaluation reports and certificates are publicly accessible.

Reference

Election Assistance Commission (EAC) website, <http://www.eac.gov/testing_and_certification/testing_and_certification_program.aspx>, accessed 16 October 2015

Venezuela

Venezuela started using electronic voting machines in 1998 (first scanners and later direct recording electronic substitutes), and currently utilizes this technology throughout the country. Biometric tools are also being implemented. While there is no certification in place, the usage of voting machines is subject to detailed scrutiny including a paper trail audit of a large percentage of the votes cast.

The source code for the electronic voting machines is reviewed before each election. Technical teams assembled by government institutions, independent institutions and political parties review the source code line by line in a 'clean room' where code can be viewed in its entirety but not modified or taken away. As part of this review process, the source code is compiled and hash values of the final versions are registered. These hash values can then be used to verify that the reviewed version of the software is being used on election day by comparing them against hash values from randomly sampled deployed voting machines.

Key features

- Source code review process accessible to interested stakeholders.
- No certification or assessments resulting in related reports.
- Limited format of the review prevents a comprehensive assessment.
- Usage of hash values helps verify that the version that has been reviewed is actually in use.

References

Carter Center, *Observing the 2006 Presidential Elections in Venezuela. Final Report of the Technical Mission* (Atlanta, GA: The Carter Center, 2007), <http://www.cartercenter.org/resources/pdfs/news/peace_publications/democracy/venezuela_2006_eng.pdf>, accessed 21 August 2015

European Union, *Final Report. Presidential Election Venezuela 2006* (Caracas: European Union Election Observation Mission, 2006), <http://eeas.europa.eu/eueom/pdf/missions/moe_ue_venezuela_2006_final_eng.pdf>, accessed 21 August 2015

Goldsmith, Ben and Ruthrauff, Holly, *Implementing and Overseeing Electronic Voting and Counting Technologies* (Washington, DC: International Foundation for Electoral Systems and National Democratic Institute, 2013), <https://www.ndi.org/files/Implementing_and_Overseeing_Electronic_Voting_and_Counting_Technologies.pdf>, accessed 16 October 2015

Martínez Dalmau, Rubén, 'Polarización política, administración electoral y voto electrónico en Venezuela', in Jordi Barrat (ed.), *El voto electrónico y sus dimensiones jurídicas: entre la ingenua complacencia y el rechazo precipitado* (Madrid: Iustel, 2015)

Annex B

Overview of relevant standards and available specifications

Product certification

CoE Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting

CoE certification of e-voting systems: guidelines for developing processes that confirm compliance with prescribed requirements and standards, 2011

CoE guidelines on transparency of e-enabled elections, 2011

VVSG 1.1, 2.0: These guidelines (mandated by the Help America Vote Act, 2002) provide a set of specifications and requirements against which voting systems can be tested to determine whether they provide all the required functionality, accessibility and security capabilities <http://www.eac.gov/testing_and_certification/voluntary_voting_system_guidelines.aspx>

Protection profiles

Bundesamt für Sicherheit in der Informationstechnik, Common Criteria Protection Profile – Basic Set of Security Requirements for Online Voting Products, 2008

Bundesamt für Sicherheit in der Informationstechnik, Digital Voting Pen, Version 1.0.1, 2007

Institute of Electrical and Electronics Engineers, P1583 SCC 38, IEEE P1583TM/D5.0: Draft Standard for the Evaluation of Voting Equipment, 2005

Lee, Kwangwoo, Yunho Lee, Dongho Won and Seungjoo Kim, Protection Profile for Secure E-voting Systems, In *Information Security, Practice and Experience*, pp. 386–97, 2010

Ministère de l'intérieur, de la securité intérieure et des libertés locales, Règlement technique fixant les conditions d'agrément des machines à voter, 2003

Quality management

ISO 9001: quality management requirements for an organization to 'say what they do, do what they say'—for example to keep documentation of procedures and perform audits to confirm that they follow the documented procedures.

ISO/TS 17582:2014: specifies requirements for the application of ISO 9001 to electoral organizations at all levels of government.

Security and functional assurance

ISO 15408 Common Criteria is a generic framework that allows computer system users to specify their security, functional and assurance requirements. Vendors can develop products and claim they meet these criteria. Testing laboratories can evaluate the products and determine whether the vendor claims are true. Common criteria are often used for critical infrastructure, as it provides assurance across the whole spectrum from the specification of requirements to product implementation and product evaluation.

ISO 27001 Information Security Management: helps organizations keep information assets secure <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm>

Expressing and communicating the separation of duties

Whether elections satisfy the relevant technical (and, consequently, legal) requirements depends on the operational context. Therefore operational requirements must be expressed and communicated precisely in an understandable manner—particularly when new technologies are introduced, because the complexity and interference of trust distributions with regard to different requirements significantly increases. The notion of *k-resilience* values (Volkamer and Grimm 2009) is one means of expressing trust distributions. In abstract terms, k-resilience values describe which entities involved in the election process are capable of ensuring the enforcement of specific requirements.

For example, from a regulatory perspective, polling station guidelines often require the application of the 'four-eyes principle' to tally votes. The accuracy

of the tallying process can then be ensured if at least one out of two poll workers operates honestly. Accordingly, the polling station arrangement is 1–of–2 resilient (it can resist the dishonesty of one of the two poll workers). A technical example is a remote electronic voting system that uses cryptographic protocols to ensure vote secrecy. Several cryptographic keys may be distributed among a number of trustees to ensure the secrecy of the vote. In this case, if at least one out of all the trustees behaves honestly, the secrecy of the vote can be ensured. If the keys are, for example, distributed among five trustees, the system would be considered 1–of–5 resilient (it can resist the dishonesty of four trustees).

K-resilience values not only apply to specific components of a system but can also be propagated to other parts. For instance, in a voting software development process, the k-resilience value expresses which vendors provide the voting system and which provide the verification system. If the same vendor provides both systems, then the accuracy of the tallying process can be ensured if one out of one vendor behaves honestly. This would be expressed as 1-of-1 resilience—the lowest resilience value, which indicates a possible single point of failure. The k-resilience value could be improved to 1–of–2 resilience if different vendors supply the voting and verification systems.

Capturing the enforcement of requirements in terms of k-resilience values with regard to different components provides a precise and understandable means of specifying the operational context. Additionally, k-resilience values might serve as a basis for communication between the EMB and stakeholders involved in the election, including the general public.

Glossary

Accreditation: a formal and independent confirmation of the competence of a certification body, which is issued by a duly authorized entity

Artefact: a verifiable product of human workmanship or skill, with neither age nor tangibility being an element thereof <http://plj.upd.edu.ph/constructing-the-past-legal-documents-as-historical-artifacts/>

Assessment: appraisal or evaluation of a system

Audit: systematic and independent examination of a system through obtaining and evaluating evidence that ensures the system fulfils pre-defined requirements; the result is a report providing third-party assurance to stakeholders

Biometric: refers to metrics related to human characteristics, such as fingerprints, hand, face, signature, voice, iris or retina

BIOS ('basic input/output system'): the basic software of a personal computer that ensures it can start up

Certification: a systematic process by an accredited body to evaluate whether a given election technology (which may include hardware, software, operation systems, management processes and personnel) satisfies previously established standards and/or legal requirements.

Certification body: an organization or company with established and verifiable competence to issue certifications, either by legal appointment or by formal accreditation according to an agreed standard

Configuration: a set of parameters that customize the settings of a computer programme, operating system or election equipment

Decryption: the process of using cryptographic methods on an encrypted computer file to make it readable (see also **Encryption**)

Discrepancy: a finding in a review process that indicates a deviation of the system under review from a defined standard against which it is being measured

Encryption: the process of using cryptographic methods on a computer file to make it unreadable to unauthorized users (related to **Decryption**)

End to end (E2E): IT processes that are run sequentially from beginning to end, used especially for systems with more than one component wherein the execution has to be performed from the end of one to the end of another

Evaluation: a key part of the overall certification process; a detailed and systematic review of the defined election technology based on set parameters

Fail-safe mechanisms: mechanisms to ensure that if a system part fails, the system responds in a way that will not cause harm to others

Feasibility study: an assessment of the practicality of a proposed project to objectively determine its strengths and weaknesses; there are several types, such as technical, economic, operational or schedule feasibility

Firmware: software that is written to the ROM of a computing device and used to run user programs on the device

Formal methods: techniques used to model complex systems as mathematical entities. By building a mathematically rigorous model of a complex system, it is possible to verify the system's properties in a more thorough fashion than by empirical testing <http://users.ece.cmu.edu/~koopman/des_s99/formal_methods/>

Hash value: a numeric value of a fixed length, which is computed using a hash function that uniquely identifies data; it is a useful tool for the examination, discovery and authentication of electronic evidence

Hashing method: an irreversible (one-way) function that allows users to unequivocally identify a message or file

Intellectual property: the legally recognized exclusive rights to creations of the mind

k-resilience: a means of expressing trust distributions to assess which entities can ensure the enforcement of specific requirements; a system is k-resilient with respect to a particular security objective if at least k entities need to operate honestly in order to achieve the security objective

Legal ductility: acceptable margin of appreciation when determining the meaning of legal terms

Legal latitude: a method of providing a fair solution when contradictory principles apply to a given case

Malapportionment: inequality arising from the unfair distribution of representatives per electoral district

Operating system: software that forms the essential base for managing the resources provided by computer hardware and software, and the management of computer programmes that 'sit on top of it'

Plebiscite: direct democracy procedure by which the citizenry of a given country expresses popular opinion on substantial topics or the continuity of political representatives

Proclamation of results: the official announcement of final election results

Proxy: an agent that acts on behalf of someone else

Requirements: a complete and detailed listing of functionalities, qualities or performance criteria that a system must comply with, which must be written in a clear, consistent, correct, feasible and verifiable manner, and which must not be open to multiple interpretations; these can be derived from standards, legal obligations originating in applicable national and international legislation, and specific objectives of the end user and other stakeholders

Review: used interchangeably with the terms 'evaluation' and 'verification' to refer to the process of validating compliance or conformity of the subject item for certification against a pre-defined set of standards

Source code: human-readable machine instructions that tell a computer system what processes and functions to perform and how to behave in specifically defined situations

Standard: a document that provides the minimum set of guidelines or characteristics that materials, products, processes and services are measured against to ensure their appropriateness for their intended purpose; they can be developed by national or international standards organizations, or formally set internally by a body for implementation and compliance purposes

Stress test: a test for reliability and stability, which tries to find the limits of a given system

System design document: a detailed written description of a system

Tabulation of votes: aggregating votes from various sources in a systematic manner

Tally: alternative term for tabulation of votes

Testing/Inspection: an investigation conducted to provide stakeholders with information about the quality of a (software) system. Testing can provide an objective, independent view of the system to allow stakeholders to appreciate and understand related risks. Test techniques include running a system to identify any deficiencies

Third-party certifier: an organization that is independent of the parties involved in the system, such as the developer, vendor and the EMB

User acceptance test (UAT): a type of testing on a system that is executed by its end user, which has to formally rate the system as 'passed' in order for it to be considered as accepted

Vendors: for-profit firms that sell proprietary voting systems to EMBs

Verification: the process of establishing the truth, accuracy or validity of a system's claims of complying with a given set of standards, guidelines and requirements, including the correctness of certification findings

Voter-verified paper audit trail (VVPAT): printed material from an electronic voting machine that shows the voter how the machine recognized his/her vote and allows the voter to confirm (or verify) his/her choices

References and Further Reading

Aaltonen, Jussi, 'Electronic Voting Case Law in Finland', in Ardita Driza Maurer and Jordi Barrat (eds.), *E-Voting Case Law: A Comparative Analysis* (Farnham: Ashgate, 2015), pp. 173–81

Barrat, Jordi, 'The Certification of E-Voting Mechanisms: Fighting Against Opacity', in Robert Krimmer and Rüdiger Grimm (eds.), *Electronic Voting 2008* (Bonn: Gesellschaft für Informatik, 2008), pp. 197–206

Barrat, Jordi, 'El voto electrónico ante intereses contradictorios: la razón comercial contra el principio democrático. A propósito de los compromisos comerciales de confidencialidad (CCC)', *Democracia digital, participación y voto electrónico* (Valencia: CEPS, 2010), pp. 57–69

Barrat, Jordi, 'The French Conseil Constitutionnel and Electronic Voting', in Ardita Driza Maurer and Jordi Barrat (eds.), *E-Voting Case Law: A Comparative Analysis* (Farnham: Ashgate, 2015)

Bock Segaard, Signe, Christensen, Dag Arne, Folkestad, Bjarte and Saglie, Jo, *Internettvalg: Hva gjør og mener velgerne?* [Internet Options: What Do the Voters Think?], (Oslo: Institutt for samfunnsforskning, 2014), <https://www.regjeringen.no/no/dokumenter/Internettvalg/id764303/>, accessed 16 October 2015

Bock Segaard, Signe and Saglie, Jo (eds.), *Evaluering av forsøket med e-valg 2011: Tilgjengelighet for velgere, tillit, hemmelig valg och valgdeltagelse* [Evaluation of the Experiment with E-Voting 2011: Accessibility for voters, trust, secrecy of the vote and voter turnout] (Oslo: Institutt for samfunnsforskning, 2012), <https://www.regjeringen.no/no/dokumenter/evaluering-av-forsoket-med-e-valg-2011/id684923/>, accessed 16 October 2015

Bundesverfassungsgericht, Decision from 3 March 2009, <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2009/03/cs20090303_2bvc000307en.html>, accessed 16 October 2015

Carter Center, *Observing the 2006 Presidential Elections in Venezuela. Final Report of the Technical Mission* (Atlanta, GA: The Carter Center, 2007), <http://www.cartercenter.org/resources/pdfs/news/peace_publications/democracy/venezuela_2006_eng.pdf>, accessed 21 August 2015

Council of Europe, *Compliance of the BeVoting Study with the Recommendation (2004) 11 of the Committee of Ministers of the Council of Europe to member states on legal, operational and technical standards for e-Voting*, (Strasbourg: Council of Europe, 2008), <http://www.elections.fgov.be/fileadmin/user_upload/Elections/fr/presentation/Compliance_Belgian_BeVoting_Rec_1_0_final_18_02_08.pdf>, accessed 25 August 2015

Election Assistance Commission [EAC] website, <http://www.eac.gov/testing_and_certification/testing_and_certification_program.aspx>, accessed 16 October 2015

Election Assistance Commission [EAC], *Voluntary Voting System Guidelines Recommendations to the Election Assistance Commission* (Washington, DC: EAC, 2007)

Election Commission of India, 'FAQs – Electronic Voting Machines', <http://eci.nic.in/eci_main1/evm.aspx>, accessed 16 October 2015

European Union, *Final Report: Presidential Election Venezuela 2006* (Caracas: European Union Election Observation Mission, 2006), <http://eeas.europa.eu/eueom/pdf/missions/moe_ue_venezuela_2006_final_eng.pdf>, accessed 21 August 2015

Federal Chancellery, *New Provisions for Online Voting: Test Conditions* (Bern: Federal Chancellery / Swiss Confederation, 2015), <https://www.bk.admin.ch/themen/pore/evoting/07979/index.html?lang=en>, accessed 15 October 2015

Federal Republic of Germany, Bundeswahlgeräteverordnung (BGBl. I S. 2459), 1975

Gesellschaft für Informatik, GI-Anforderungen an Internetbasierte Vereinswahlen, 2005, <https://www.gi.de/fileadmin/redaktion/Wahlen/GI-Anforderungen_Vereinswahlen.pdf>, accessed 16 October 2015

Goldsmith, Ben and Ruthrauff, Holly, *Implementing and Overseeing Electronic Voting and Counting Technologies* (Washington, DC: International Foundation for Electoral Systems and National Democratic Institute, 2013), <https://www.ndi.org/files/Implementing_and_Overseeing_Electronic_Voting_and_Counting_Technologies.pdf>, accessed 16 October 2015

Gugliemi, G. and Ihl, O. (eds.), *Le vote électronique* [The Electronic Vote] (Paris: LGDJ, 2015)

Institute of Electrical and Electronics Engineers [IEEE], P1583 SCC 38, IEEE P1583TM/D5.0, *Draft Standard for the Evaluation of Voting Equipment*, 2005

International Association for Cryptologic Research, *Requirements and Evaluation Criteria*, 2015, <http://www.iacr.org/elections/eVoting/requirements.html>, accessed 16 October 2015

International IDEA, *The Use of Open Source Technology in Elections* (Stockholm: International IDEA, 2014)

Karokola, Geoffrey, Kowalski, Stewart and Yngström, Louise, 'Secure e-Government Services: Protection Profile for Electronic Voting: A Case of Tanzania', *Proceedings of the IST-Africa 2012 Conference*, 2012

Katholieke Universiteit Leuven, Universiteit Antwerpen, Universiteit Gent, Université Catholique de Louvain, Université de Liège, Université Libre de Bruxelles and Vrije Universiteit Brussel, *BeVoting Study of Electronic Voting Systems Part I* of the 'Studie Geautomatiseerde Stemming Def. Vs 18122006', 15 April 2007, <http://www.elections.fgov.be/fileadmin/user_upload/Elections/fr/presentation/bevoting-1_gb.pdf>, accessed 25 August 2015

Katholieke Universiteit Leuven, Universiteit Antwerpen, Universiteit Gent, Université Catholique de Louvain, Université de Liège, Université Libre de Bruxelles and Vrije Universiteit Brussel, *BeVoting Study of Electronic Voting Systems Part II* of the 'Studie Geautomatiseerde Stemming Def. Vs 18122006', 4 December 2007, <http://www.elections.fgov.be/fileadmin/user_upload/Elections/fr/presentation/bevoting-2_gb.pdf>, accessed 25 August 2015

Kiesraad, *Supporting Software Elections*, <http://kiesraad.nl/artikel/ondersteunende-software-verkiezingen-osv>, accessed 16 October 2015

Krimmer, Robert and Ehringfeld, Andreas and Traxl, Markus, *E-Voting bei den Hochschülerinnen— und Hochschülerschaftswahlen 2009. Evaluierungsbericht* (Vienna: Austrian Federal Ministry of Science and Research, 2010), <http://www.e-voting.cc/wp-content/uploads/downloads/2015/04/Evaluierung_OeH-Wahl_E-Voting.pdf>, accessed 15 October 2015

Kuoni, Beat, 'E-Voting Case Law: A Swiss Perspective', in Ardita Driza Maurer and Jordi Barrat (eds.), E-*Voting Case Law: A Comparative Analysis* (Farnham: Ashgate, 2015)

Lee, Kwangwoo, Lee, Yunho, Won, Dongho and Kim, Seungjoo, 'Protection Profile for Secure E-voting Systems', in Chen, K., Deng, R., Lai, X. and Zhou, J. (eds.), *Information Security, Practice and Experience* (Berlin and Heidelberg: Springer, 2010)

Martínez Dalmau, Rubén, 'Polarización política, administración electoral y voto electrónico en Venezuela', in Jordi Barrat (ed.), *El voto electrónico y sus dimensiones jurídicas: entre la ingenua complacencia y el rechazo precipitado* (Madrid: Iustel, 2015)

Ministère de l'intérieur de la securité intérieure et des libertés locales, *Règlement technique fixant les conditions d'agrément des machines à voter*, 2003

National Democratic Institute [NDI] and International Foundation for Electoral Systems [IFES], *Implementing and Overseeing Electronic Voting and Counting Technologies* (Washington, DC: NDI and IFES, 2013), <https://www.ndi.org/files/Implementing_and_Overseeing_Electronic_Voting_and_Counting_Technologies.pdf,> accessed 16 October 2015

Neumann, Stephan and Volkamer, Melanie, 'A Holistic Framework for the Evaluation of Internet Voting Systems', *Design, Development, and Use of Secure Electronic Voting Systems* (2014), pp. 76–91

Ordinateurs de vote, <http://www.ordinateurs-de-vote.org>, accessed 16 October 2015

Organization for Security and Co-operation in Europe/Office for Democratic Institutions and Human Rights, 'Elections in Belgium', <http://www.osce.org/odihr/elections/belgium>, accessed 16 October 2015

– 'Elections in Estonia', <http://www.osce.org/odihr/elections/estonia>, accessed 16 October 2015

– 'Elections in France', <http://www.osce.org/odihr/elections/france>, accessed 16 October 2015

– 'Elections in Norway', <http://www.osce.org/odihr/elections/norway>, accessed 16 October 2015

– 'Elections in Switzerland', <http://www.osce.org/odihr/elections/switzerland>, accessed 15 October 2015

– *Handbook for the Observation of New Voting Technologies* (OSCE/ODIHR, 2013), <http://www.osce.org/odihr/elections/104939?download=true>, accessed 16 October 2015

Philipps, Mark and Soudriette, Richard, 'Testing Democracy: How Independent Testing of E-Voting Systems Safeguards Electoral Integrity', *Electronic Voting 2012* (Bonn: Gesellschaft für Informatik, 2012), <http://www.e-voting.cc/wp-content/uploads/downloads/2012/07/159-170_Soudriette-Phillips_Testing-Democracy.pdf>, accessed 16 October 2015

PourEva, 'Expert Reports', <http://www.poureva.be/spip.php?rubrique19>, accessed 16 October 2015

PP-CIVIS, *Protection Profile: Profil de Protection Machine à voter*, 2006, <http://www.ssi.gouv.fr/archive/site_documents/pp/pp0604.pdf>, accessed 16 October 2015

Prasad, Hari K. et al., 'Security Analysis of India's Electronic Voting Machines', *Proceedings of the 17th ACM Conference on Computer and Communications Security* (Chicago: ACM, 2010), <https://indiaevm.org/evm_tr2010-jul29.pdf>, accessed 16 October 2015

Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Harri, H., MacAlpine, M. and Halderman, J. Alex, 'Security Analysis of the Estonian Internet Voting System', *Proceedings of the 21st ACM Conference on Computer and Communications Security* (Scottsdale: ACM, 2014), <https://jhalderm.com/pub/papers/ivoting-ccs14.pdf>, accessed 16 October 2015

Stenerud, Ida, Gebhardt, Sofie and Bull, Christian, 'When Reality Comes Knocking: Norwegian Experiences with Verifiable Electronic Voting', in *Electronic Voting 2012* (Bonn: Gesellschaft für Informatik, 2012)

Vähä-Sipilä, Antti, *A Report on the Finnish E-Voting Pilot* (Helsinki: Electronic Frontier Finland, 2009), <http://www.effi.org/system/files?file=FinnishEVotingCoEComparison_Effi_20080801.pdf>, accessed 20 August 2015

Vegas González, Carlos, 'The New Belgian E-voting System', in *Electronic Voting 2012* (Bonn: GesellschaftfürInformatik, 2012), pp. 199–211, <http://www.e-voting.cc/wp-content/uploads/downloads/2012/07/199-211_Vegas_Belgian-E-voting.pdf>, accessed 16 October 2015

Victorian Electoral Commission, 'EAV Detailed Information', <http://www.vec.vic.gov.au/Voting/ElectronicVotingDetail.html>, accessed 16 October 2015

Volkamer, Melanie, *Evaluation of Electronic Voting* (Berlin and Heidelberg: Springer, 2009)

Volkamer, Melanie and Grimm, Rüdiger, 'Determine the resilience of evaluated internet voting systems', *Requirements Engineering for e-Voting Systems* (RE-VOTE), 2009 First International Workshop, IEEE, 2010

Whitmore, Keith, *Information Report on the Electronic Voting in the Finnish Municipal Elections Observed on 26 October 2008* (Strasbourg: Congress of Local and Regional Authorities, 2008)

About the Contributors

Contributors

Jordi Barrat is Professor of Public Law at the University of Catalonia/URV. His research is focused on how legal regulations may enhance political participation, in particular how new technologies are being deployed in the electoral field. He also served as Deputy of the Catalan Office for the Quality of Democracy, a governmental innovation unit, and has joined international assistance missions on behalf the Council of Europe, IFES, OSCE/ODIHR and OAS. He holds a PhD in Public Law [León (Spain)].

Eden Bolo is an IT Officer at the Philippine Commission on Elections. She has provided technical support and management assistance for Philippine automated voter registration systems since 1993 and automated election systems since 1994, including system requirements definition, systems evaluation and testing, and systems preparation, implementation and monitoring. She is currently a member of the independent Technical Evaluation Committee, which is mandated to certify the automated election system for use in the May 2016 elections.

Alejandro Bravo is a Specialist in the Department of Electoral Cooperation and Observation (DECO) at the Organization of American States. He works in the areas of technical cooperation, election technology, audit of electoral registries, information security, project management and election observation, and has created software for technical electoral cooperation management. He holds an MS from George Washington University. DECO provides technical support to electoral bodies in the implementation of quality management systems and certification against ISO standards. In February 2014, supported by the OAS, the first-ever ISO International Electoral Standard, ISO/TS 17582: 2014 was published.

Robert Krimmer is Professor of e-Governance at the Tallinn University of Technology, Estonia. His research focuses on the transformation of the public sector, electronic democracy and related issues. He previously served as Senior Adviser on New Voting Technologies in the Election Department of the OSCE's Office for Democratic Institutions and Human Rights (OSCE/ODIHR), in Warsaw, Poland. His role was to coordinate and support the use of new technologies in election-related activities and to help develop the relevant methodology. Dr Krimmer has been part of the work of the CoE on its Recommendation Rec(2004)11 on Electronic Voting from the very beginning, he founded and chairs E-Voting.CC, and he initiated the bi-annual EVOTE conference series held in Bregenz, Austria. He holds an MBA from the WU Vienna University of Economics and Business and a PhD from the Tallinn University of Technology.

Stephan Neumann is a Research Associate and doctoral student at Technische Universität Darmstadt, where he focuses on information security and secure electronic voting. Mr Neumann has contributed to more than 20 publications and has presented his research results at several international conferences. He has been a member of several programme committees and holds an MSc from Saarland University.

Al A. Parreño is a Commissioner in the Philippine Commission on Elections, where he is in charge of the technology training and the technology capability pillar, the Office for Overseas Voting and security assessments. He was previously a member of the Land Transportation Franchising and Regulatory Board, where he was in charge of land franchise management and logistics.

Carsten Schürmann is Associate Professor at the IT University of Copenhagen, where he researches information security, cryptography, language-based security, formal methods and computational social choice. He leads the DemTech research project on trustworthy democratic technologies, an interdisciplinary research effort between computer science and social science that studies trust in digital elections. He consults with electoral management bodies regarding the design of voting protocols. Since 2015 he has served as a member on the IEEE VSSC1622 voting systems standards committee of the working group on Voting Methods Mathematical Models. In 2002, he received the NSF CAREER award. He holds a PhD from Carnegie Mellon University.

Melanie Volkamer is Assistant Professor at Technische Universität Darmstadt, where she leads the Security, Usability, and Society (SECUSO) research group, and a part-time Associate Professor at the Karlstad University. She has been an advisory board member of many e-voting projects and initiatives. In particular, she acted as an OSCE election observer at the first parliamentary remote electronic election in Estonia in 2007. Furthermore, she was invited

by the German Federal Constitutional Court to serve as a technical expert for e-voting in 2008. Dr Volkamer has presented her research at numerous conferences and to many organizations including the Council of Europe. She has co-authored two Common Criteria Protection Profiles for electronic voting and holds a PhD from the University of Koblenz.

Peter Wolf is a member of the Elections Processes Programme at International IDEA. He has focused on ICT applications in electoral processes since joining the Elections Department of the OSCE mission in post-war Bosnia and Herzegovina, where he worked on voter registration and results databases. He served as a consultant in voter registration projects in Albania, DR Congo and Iraq, and participated in various International Election Observation Missions, including as an electronic voting expert in France, Kazakhstan, Kyrgyzstan, Venezuela and the Philippines. He holds an MS from the Graz University of Technology.

About International IDEA

The International Institute for Democracy and Electoral Assistance (International IDEA) is an intergovernmental organization that supports sustainable democracy worldwide. International IDEA's mission is to support sustainable democratic change by providing comparative knowledge, assisting in democratic reform, and influencing policies and politics.

What does International IDEA do?

In the fields of elections, constitution-building, political parties, gender in democracy and women's political empowerment, democracy self-assessments, and democracy and development, International IDEA works in three main activity areas:

- providing comparative knowledge derived from practical experience on democracy-building processes from diverse contexts around the world;
- assisting political actors in reforming democratic institutions and processes, and engaging in political processes when invited to do so; and
- influencing democracy-building policies through the provision of comparative knowledge resources and assistance to political actors.

Where does International IDEA work?

International IDEA works worldwide. Based in Stockholm, Sweden, it has offices in Africa, Asia and Latin America.

When introducing or using information and communications technologies (ICTs) in elections, electoral management bodies (EMBs) usually need to assure themselves and other stakeholders that a given technical solution is going to work—that is, that it fulfils legislated requirements, is secure and trustworthy, is of high quality, and will perform as expected.

Certification of ICTs for use in elections is often seen as an option for EMBs seeking to provide this kind of assurance. However, certification practice varies greatly between countries and EMBs. Some do not conduct any kind of certification, while others use very distinct processes with vast differences in scope. Further complicating matters is the fact that certification terminology is badly defined and applied inconsistently. Moreover, as there is currently no global technical standard for the various ICTs used in electoral processes it is usually up to the individual EMB to develop requirements for the certification process and assure compliance.

This publication provides guidance on what the certification of ICTs for elections can and cannot achieve, outlines the relationship between the legal and technical requirements for certification, and presents a quality-assurance framework that summarizes best practices for planning and implementing certification.

International IDEA
Strömsborg, SE–103 34, Stockholm, Sweden
Tel: +46 8 698 37 00, fax: +46 8 20 24 22
info@idea.int
www.idea.int

ISBN: 978-91-7671-028-9