WOTE 2006 Contribution

Paper on

an Electronic Electoral Services Accreditation Framework

and

Developments of the required

Standards

Date: 1St June 2006

Prepared by: John Ross
Director

Security and Standards Consultancy Ltd
The Waterhouse Business Centre
2 Cromar Way
Chelmsford,
Essex
England, UK
Tel:+44 (0)7771970805
ross@secstan.com

Abstract

To meet the challenges of trustworthy elections conducted with the aid of electronic voting components and system, fundamentally the electronic systems not only needs to be trusted, but also needs to be seen as trustworthy, by the voting population. There is always the need for public verifiability of the whole voting process and this is particularly true when electronic voting components/systems are used to assist public voting within a democracy.

The electronic voting components whether they are; stand alone paper e-counting systems, "Direct Recording Electronic" voting machine or fully integrated e-voting systems, require trust to be placed in those components and systems. This paper postulates that building such trust will not happen unless there is a measured way to assess, certify and accredit the electronic components used in the election process.

This paper proposes the development of Electronic Electoral Services Accreditation Framework, similar to the accreditation frameworks used to assess, certify and accredit electronic security systems but tailored specifically to meet the unique needs of electoral systems and services. The paper draws on several activities the author has been involved with over the last few years, including being one of the editors of the Electronic Mark-up Language of OASIS, the editor of contributions to Council of Europe Recommendation Rec (2004)11 Legal, Operation and Technical Standards for e-voting and as a leading member of an Electronic Electoral Services Accreditation, Assessment and Certification Feasibility Study for a UK government department.

Introduction

The deployment of electronic electoral systems/services (i.e. e-voting/e-counting systems) for public elections in modern democracies must take a rigorous approach to ensuring their security and trustworthiness, and must be seen to be taking a rigorous approach. Openness to public scrutiny of any electronic election service will be a vital factor in it achieving public acceptability.

The establishment of an Accreditation, Assessment and Certification framework for electoral systems and services – referred to as an Electoral Assurance Framework - provides a mechanism to achieve this. It would provide an independent way of ensuring that systems meet the electronic electoral service requirements and reduces the risk of deploying inappropriate systems, selecting unsuitable service providers and perhaps more critically, acting upon invalid results. Establishing a Electoral Assurance Framework would:

- Provide an essential foundation for the deployment of electronic systems/services within public elections.
- Provide enhanced confidence in electronic electoral systems/services.
- Save money. Without an Assurance Framework, electoral systems/services would need to be assessed on an individual basis for each election. The aggregate cost of assurance across all the systems for all elections would be very high. If, however, an Electoral Assurance Framework is established, whereby election systems can be certified as having been assessed, then significant savings can be made. Whilst the initial cost of the certified systems may be higher, the savings made by no longer needing to repeatedly assess the systems in detail for individual elections would more than offset the higher cost of certified systems.

- Ease the procurement burden on governments and administrators seeking to implement Electronic Electoral Services through the development of clear requirements and prior evaluation of systems against these requirements.
- Ease the process of quality assurance during the short timescales available during the run up to an election.
- Provide stability and potentially growth in the electronic electoral market through the availability of clear requirements and accreditation needs of electronic electoral systems/services that could apply internationally.

Electoral services being assured need to support all types of public elections, including national government elections on an international stage. Electoral services need to be delivered on an international bases and assessed in accordance with internationally agree standards and practices.

Process model for Election Events

To define how an Electoral Assurance Framework could be used to deliver confidence in electronic electoral services, a high level process model for Elections needs to be defined. This model needs to cover all the aspects involved in establishing, operating, tallying and verifying an election.

A process model is used in the OASIS EML standard to establish potential interoperability requirements within e-voting systems and services. These interoperability points can therefore be openly specified and used as scrutiny points within the whole voting process. Such points can be openly assessed, verified and product offering such interface points can be tested and certified under the Electoral Assurance Framework. The EML model defines processes that are common to almost any Election Event in our modern democracies. As shown in the figure, there are the following major processes:

a. voter registration (shaded in dark yellow in the figure);

b. candidate management (shaded in dark purple in the figure);

c. election (including ballot) preparation (shaded in light purple in the figure);

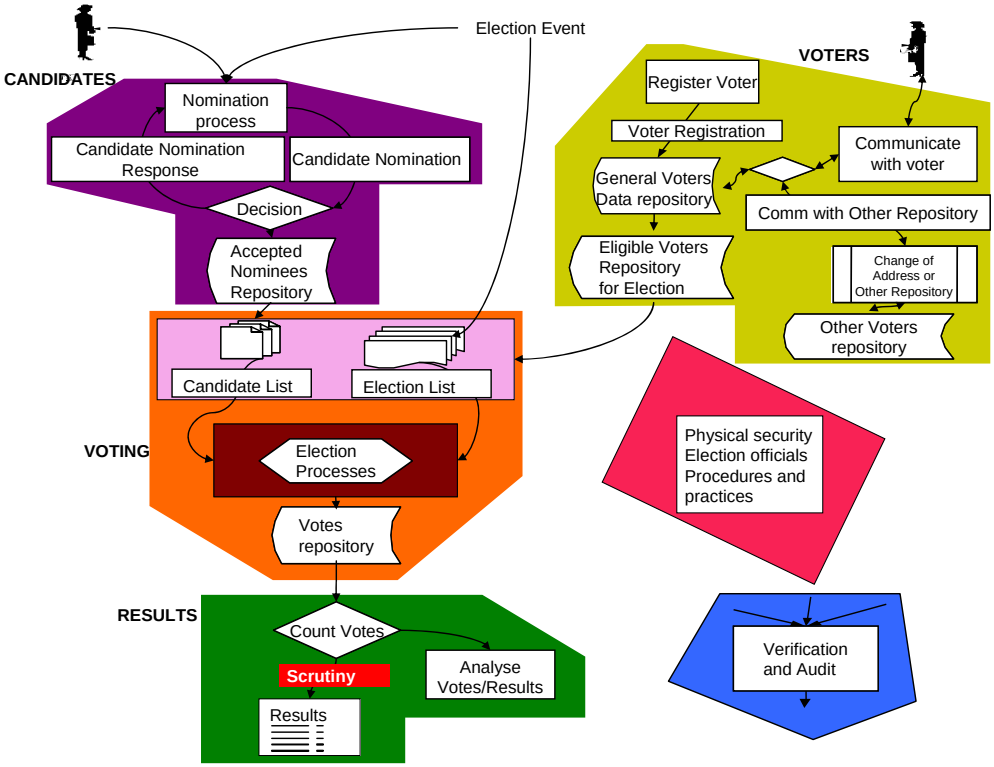
d. voter’s selection (shaded in brown in the figure);

e. vote lodging (shaded in orange in the figure);

f. counting and results (shaded in green in the figure);

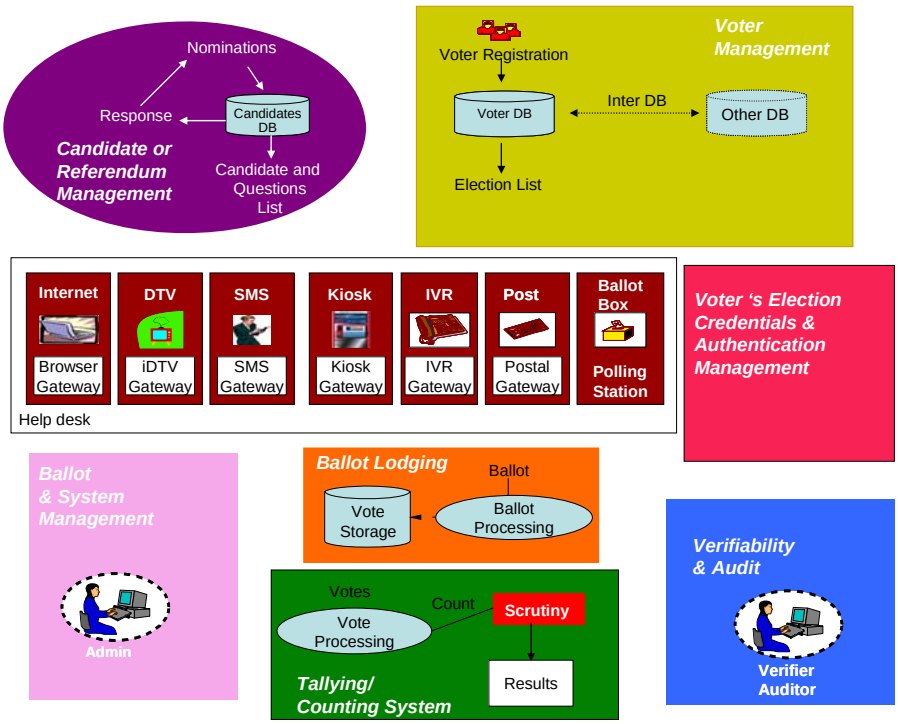
g. verification and audit (shaded in blue in the figure);

h. election security (shaded in red in the figure).



Model for Election Processes and Systems

By analysing the process model illustrated above the possible electronic electoral functional areas can be identified. These are shown below, the figure has been colour coded to show which process each functional area is supporting. The colours are the same as those used in Figure above.

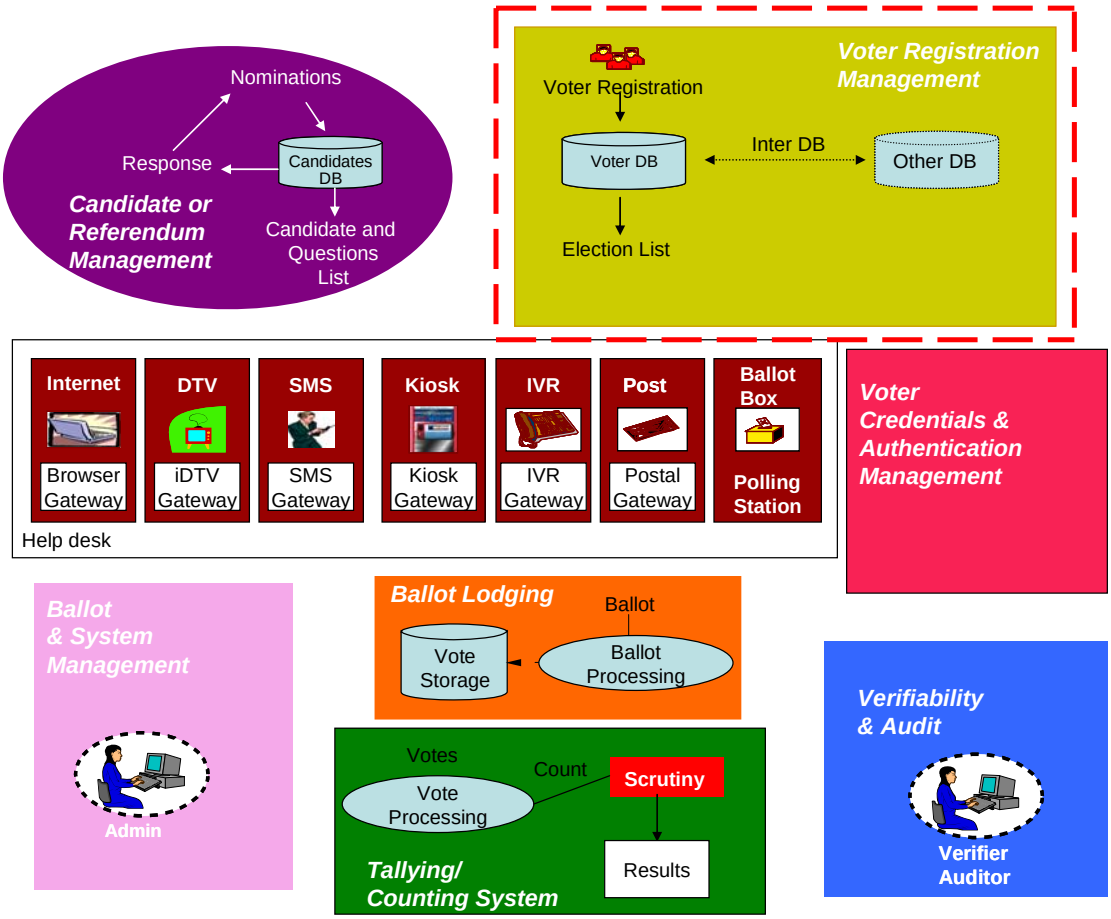


- The model allows for a mixture of automated and manual process as part of an overall electronically assisted election event, the Electoral Assurance Framework needs be able to assess and establishment trust and confidence across all the areas identified in the model, covering both the manual and electronic processes. An electronic electoral component, systems or service may fulfil or assist in one or more of these processes, for example standalone electronic registration system may assist in the registration process. On the other hand a sophisticated e-voting systems may assist in:
  - The distribution of voters tokens or credentials,
  - The process of casting votes, gathering, securing, recoding and counting votes,
  - The verification and auditing processes to ensure the result is true, sound and assist in any enquires or investigations.

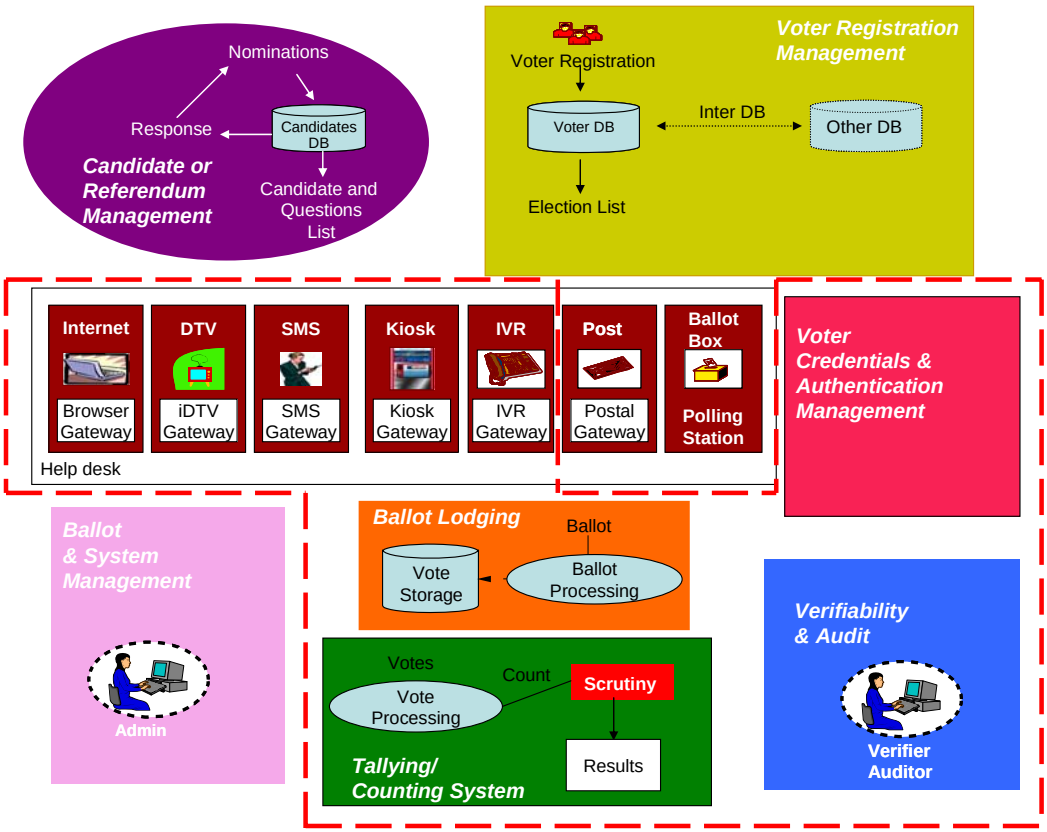
Sample Electoral Systems

Illustrated below are electoral functions which can be provided, or assisted, by two sample systems; an electronic Registration systems and an e-voting system.

The functions that could be provided or assisted by electronic registration system are those within the red dashed box.



The functions that could be provided or assisted by electronic e-voting system are those within the red dashed box.



Aspects of an Electoral Assurance Framework

The aspects of an electoral assurance framework are:

- Points of assessment:

  Establish the points at which assessments could be undertaken, ranging from the time of an election only, the time at which election systems have been brought together and the assessment of components and products during their development and maintenance;

- Confidence and Trust levels

  Establish the required level of confidence that stakeholders require the Assurance Framework to deliver and the trust levels needed in dedicated components

- Risk management

  Identify the key risks and exposures by means of a risk analysis.

To ensure cost effective evaluation, inspection activities should be targeted at the highest risk/critical components of the system, thus there is a need for a risk based approach.

The supporting documentation to the Council of Europe (COE) recommendations includes a threat analysis, this analysis identifies the threats to an electronic voting system during each of the following stages of an election:

- Pre-voting;
- Voting;
- Post-voting.

This COE threat analysis is based on abstract model and needs to be applied within the context of real systems vulnerabilities where the impact of the threat can be assessed as being critical. Using a risk management approach assessments can be targeted at the most critical components of the system. Using the COE threat analysis on example configurations of real systems one can determine the probable impact levels of the consequences of a failure of security within those systems or its components. This in turn leads on to being able to quantify the degree (depth/vigour) of assessment that each components needs to be assessed under the framework.

Example Impact Assessments

Illustrated in the table below is a summary of impact levels based on applying the COE risk assessment to real electoral systems/components with real assessment points that cover the various functional areas of voting systems illustrated in the multicoloured diagram above.

Real Systems/Components	**COE Impact Stage**	**Probable Impact level**
e-Voting	Pre voting , Voting and Post-Voting	Very High
Registration	Pre voting	Low
Election Management	Pre voting, Voting	Medium
Authentication	Voting	High
Unsupervised e-voting channels	Voting	Very High
Supervised channels	Voting	Medium/High
Vote lodging	Voting	High
Tally/counting	Voting , Post voting	Very High
Verification and audit	Pre voting , Voting and Post-Voting	Very High

Based on the above impact levels, the components that need the greatest depth (vigour) of assessment under the framework would be

- Unsupervised Channels system/components
- Tally/counting systems/components
- Verification and audit system/components

The next highest would be vote lodging and authentication/credential management systems/components.

This does not imply that no assessment is required in the rest of the components, only the type and level of assessment (vigour) needed in these components is possibly less.

Conclusion

This paper concludes that setting up an Electoral Assurance Framework is the only way to provide a high level of confidence in deployment of the electronic electoral system. Assuming the wide scale adoption of electronic voting, it is also likely to save money in the longer term. It will reduce the risks of running elections by delivering higher assurance systems and reduce the skill required of the assessor at the time of the election.

An Electoral Assurance Framework should seek to obtain high confidence in the correct operation of the e-voting systems. Going for a lower confidence level, while reducing the assessment and certification costs, is likely either not to be cheaper over the whole life of the election system or to result in significantly higher risk of electoral fraud. The reduced cost associated with election time assurance activities with certified products/services more than compensates for the cost associated with certification of the products/services themselves.

An Accreditation scheme could initially be based on performing assessment activities at election and system level assessment points with targeted component assessment. While offering slightly less assurance than performing full assessment of all election components it will provide cost savings.

Standards are needed for such an Assurance Framework to function, these need to be developed over the next few years. A lot can be leant from the standards for IT security assurance, but IT security standards do not address the specific requirements of electoral systems. Dedicated standards are needed that specifically address the needs of e-voting systems.

Ideally the standards needed for an Electoral Assurance Framework should be developed on an International basis, so that the assessment and certification applies to common standards across the democratic world.

The OASIS EML standard defines open interfaces between the various process involved in elections and electoral management, such open XML interfaces can provide convenient points at which the Electoral Assurance Framework can assess the various components of electoral systems. The degree (vigour) of the assessment required can be made appropriate to impact of a security problem with a particular component of an electoral system/service and hence establish the level of trust that can be required/placed in that component.

Standardised interface points provide by the OASIS EML standard also provide the ability to employ multiple trust paths within an electoral systems. Thus as an example, standard auditing interfaces could enable the electoral verification and audit systems to be totally independent from other parts of the electronic electoral system giving rise to trusted vote auditing processes which could be independently assessed and certified under the Electoral Assurance Framework.