Workshop on UOCAVA Remote Voting Systems

OASIS Election & Voter Services

Technical Committee

Position Paper

Submitted 26 July 2010

Introduction

This paper is submitted in response to the call for papers for the workshop on UOCAVA Remote Voting Systems. It seeks to address the following topics from the full list of topics published for the workshop:

- Desired/required functional properties of UOCAVA remote voting systems;
- Risks associated with using the Cyber Infrastructures such as the Internet;
- Risks associated with remote electronic voting;
- Experiences with remote electronic absentee voting systems.

Challenges

On-line services are becoming an everyday occurrence and government services are increasingly becoming available in remote, unsupervised situations. The question is, “Can remote, unsupervised voting also be made available?” The benefits of such convenience are clear, but the unique requirements and critical role of elections in civic life make implementation a challenge. A general assessment of concerns, risks, and mitigation strategies can be found in Appendix B of the Election Markup Language (EML) v6.0 Specification document (www.oasis-open.org/committees/document.php?document_id=38333&wg_abbrev=election).

Since democracy was invented, people have sought ways to illicitly influence the outcome of a vote. When e-enabled voting systems are used, an important goal must be to reduce the risk of cheating, especially in ways that were not available in non-electronic systems. In addition, for UOCAVA voters, the aim should also be to provide better, simpler access to voting, along with the re-assurance of trust and security in the process.

To build trust in a voting system, people need to understand how their personal information and votes are handled. Moreover, the ability to independently verify the integrity of the system and accuracy of its results go a long way to building confidence in a system.

We present the following brief comparison of online banking and online voting to illustrate how they differ from each other conceptually and in practice. The key points to note are:

- It is all about verification and what a human is able to physically and tangibly know and prove compared to what a computer can make a human think they just saw happen;
- Anonymous voting and vote tallying is 180° opposite of banking where every transaction is tied to a specific customer/receipt/recipient;
- Anonymous voting requires that the voter cannot be identified and their specific vote known;
- Voter intimidation and vote selling are illegal.

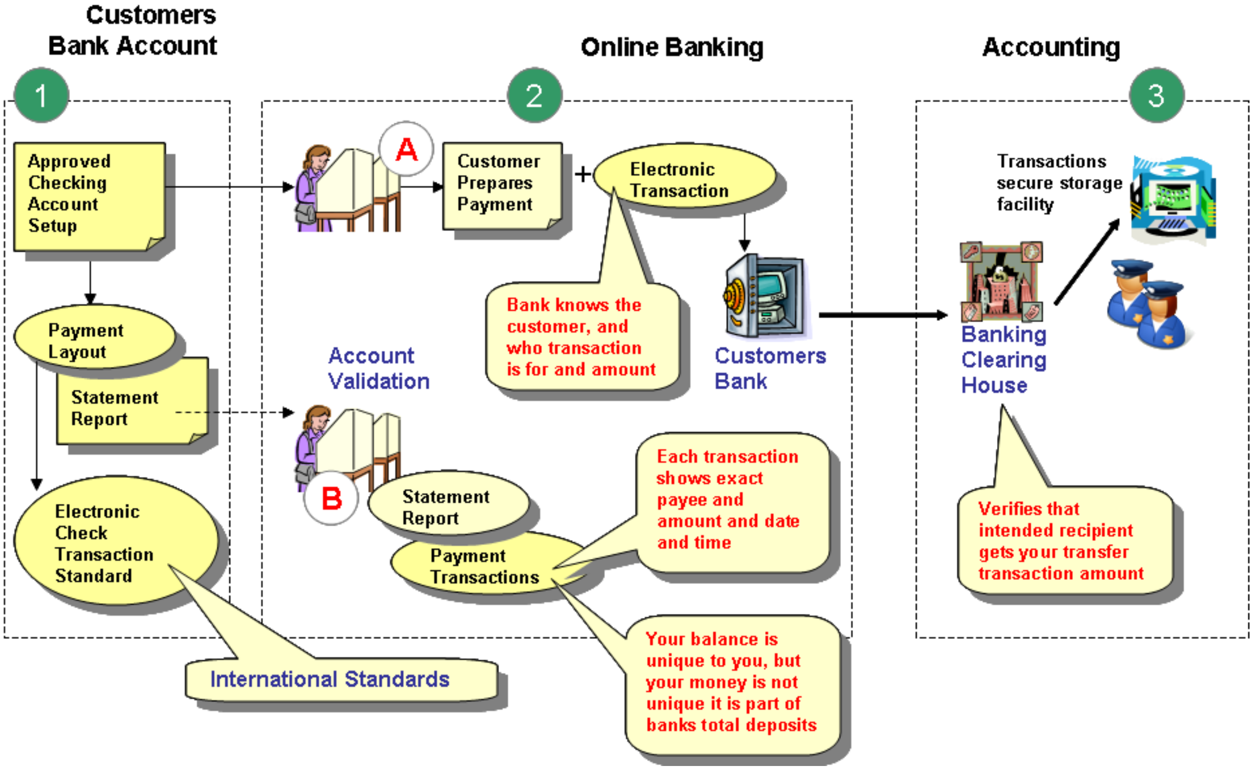
Customers Bank Account
Online Banking
Accounting
1
2
3
Approved Checking Account Setup
A
Customer Prepares Payment
+
Electronic Transaction
Transactions secure storage facility
Bank knows the customer, and who transaction is for and amount
Payment Layout
Statement Report
Account Validation
Customers Bank
Banking Clearing House
B
Statement Report
Each transaction shows exact payee and amount and date and time
Electronic Check Transaction Standard
Payment Transactions
Verifies that intended recipient gets your transfer transaction amount
International Standards
Your balance is unique to you, but your money is not unique it is part of banks total deposits

Figure 1 illustrating aspects of online banking

Then for comparison Figure 2 shows online voting.

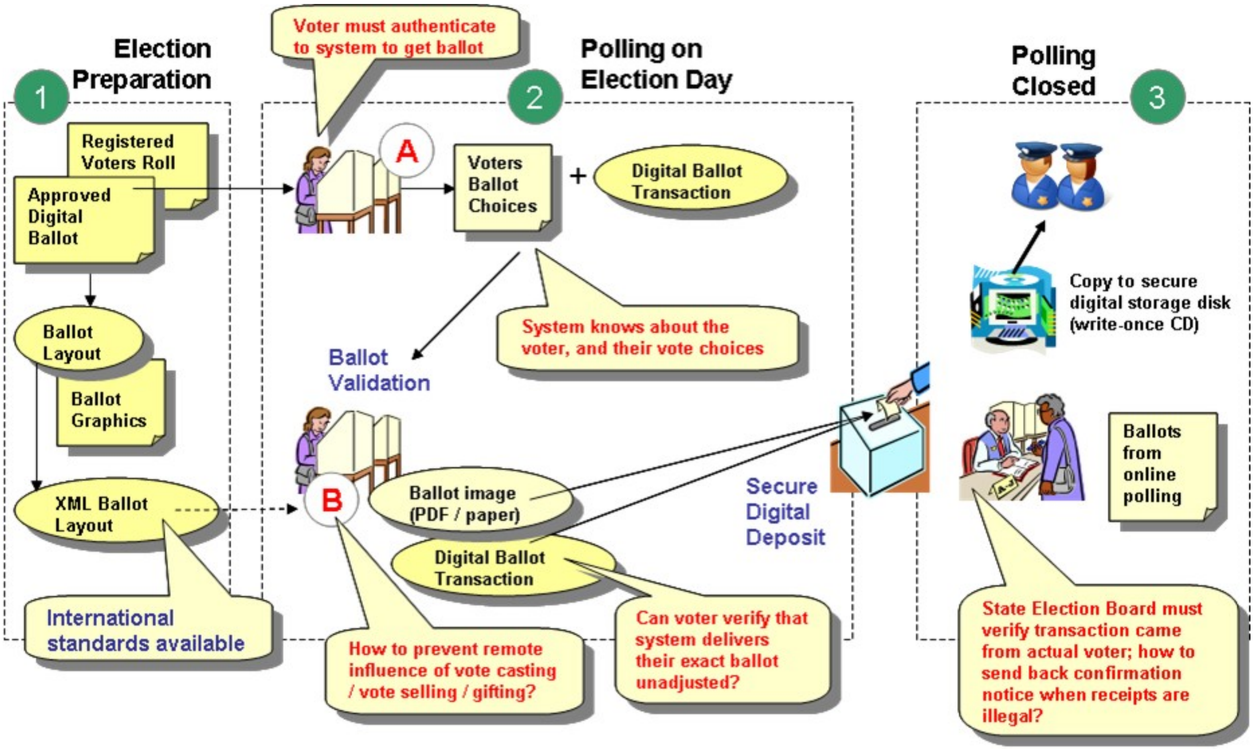
Voter must authenticate to system to get ballot
Election Preparation
Polling on Election Day
Polling Closed
1
2
3
Registered Voters Roll
Approved Digital Ballot
A
Voters Ballot Choices
+
Digital Ballot Transaction
Copy to secure digital storage disk (write-once CD)
Ballot Layout
System knows about the voter, and their vote choices
Ballot Validation
Ballot Graphics
Ballots from online polling
XML Ballot Layout
B
Ballot image (PDF / paper)
Secure Digital Deposit
Digital Ballot Transaction
International standards available
How to prevent remote influence of vote casting / vote selling / gifting?
Can voter verify that system delivers their exact ballot unadjusted?
State Election Board must verify transaction came from actual voter; how to send back confirmation notice when receipts are illegal?

Figure 2 illustrating aspects of online voting

Key Functional Properties

We recognise, in no particular order, the following key functional properties of a remote, unsupervised voting system.

- Election officials can determine that a submitted vote is associated with a unique right to vote (vToken), which has been issued in a way that it is disassociated from the individual voter;
- The voter can independently verify their ballot vote details;
- The election process has safeguards against a vote being sold, gifted or influenced; e.g. a voter can recast their ballot after the influence has been eliminated;
- A voter can verify that their actual ballot choices have been cast;
- Election officials can confirm ballots came from real voters physically submitting ballots and not computer emulation of voters;
- It is possible to conduct a full audit of the process.

For background on the functional properties listed above, we reference the Council of Europe (CoE) Recommendation on standards for e-voting (www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/Default_en.asp). These standards were drawn up by legal experts, operational experts, and election officials, and then agreed to by Ministers from all Members States of the CoE. EML supports all of the standards set down in this Recommendation and we would suggest that UOCAVA systems adhere as closely as possible to this Recommendation.

There are various ways that the above functional properties can be achieved and, indeed, whether they are all even necessary in a UOCAVA environment. As a standards committee, our role is to provide technical support for whatever methods are used. We can demonstrate to EAC/FVAP/NIST how EML can support each of the functional properties.

Other Key Aspects of eVoting Systems

An *Electoral Assurance Framework* allows independent assessment of an election system.

An Electoral Assurance Framework:

- Builds trust by enabling public verifiability of the whole voting process;
- Is based on open standards;
- Provides standardised interface points where vote auditing processes can be independently assessed;
- Allows accreditation, assessment and certification of electoral systems and services.

Transparency and auditability are key aspects of the framework. Well-defined, open interfaces can provide transparency for the whole voting process, from the time the votes are cast to the final count. Full-scale deployment of systems within an Electoral Assurance Framework promotes:

- Voter anonymity and vote secrecy;
- Election verifiability and auditability;
- Trust in the system.

The OASIS EML Standard

EML has been developed over a number of years as a standard for the structured interchange of data among hardware, software, and service providers. These providers deliver election and voter services to public and private organizations. The objective has been to introduce a uniform and reliable way for components of an election system to interoperate. It incorporates the global experiences and knowledge of a wide range of election system practitioners and suppliers.

EML provides specifications that:

- Are an open, public, international standard;
- Provides a complete multi-lingual suite of election and voting management transactions;
- Ensures consistent representation of voter records, election, districts, ballots & votes;
- Supports verifiable transactions, including digital signatures and vTokens (voting entitlement/device) ;
- Have been used for all aspects of e-Voting

Experiences

We offer the following list as examples of current and recent remote voting pilots/systems:

France - remote voting for non-resident French citizens became available last year. A report is available at www.edemocracy-forum.com/2009/07/frencevoting2009.html#more

Holland – remote voting for non-resident Dutch citizens has been available over the last couple of years. See Section 7 of the report of the Second meeting to Review developments in the field of e-voting since the adoption of Recommendation Rec(2004)11 (Madrid, 16 October 2008) available at www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/Default_en.asp

Switzerland – various Cantons in Switzerland are in the process of conducting e-voting pilots, particularly for non-residents. A report on their activities is available at “National reports on developments in the field of e-voting” at www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/Default_en.asp

UK – the UK has conducted two series of e-voting pilots over the last few years and reports on both are available at www.justice.gov.uk/guidance/may2007electoralmodernisation.htm.

Summary

Open standards are the base on which to build trustworthy, open, and creditable e-enabled elections. Using consistent data and exchanging that data at recognised interface points is essential for trusted elections. EML comprehensive in scope and is the only available international. open standard that meets the needs of elections officials and voters.

In addition the following should be noted:

- EML provides a consistent verifiable way to represent an election digitally;
- EML enables public result reporting and auditing records;
- Remote, unsupervised voting services can be enhanced by using OASIS EML as it provides a range of proven supporting mechanisms.