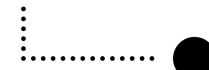




Berner Fachhochschule



Technik und Informatik

Election Markup Language Overview

Stephan Fischli

Introduction (1)

Organization

- OASIS XML Interoperability Consortium
- Election and Voter Services Technical Committee

Mission

- Standard for the structured interchange among hardware, software, and service providers who engage in providing election or voter services to public or private organizations

History

- Formation in March 2001
- Interoperability demonstration in October 2007
- Release of version 5.0 in December 2007

Introduction (2)

Deliverables

- Set of data and message definitions as XML schemas
- Generic election process model (requirements, data dictionary)

Related Work

- Council of Europe ad hoc Committee on e-Democracy (CAHDE)
- UK CORE Project (Co-ordinated Online Register of Electors)
- IEEE Voting Systems Electronic Data Interchange
- Open Voting Consortium (OVC)

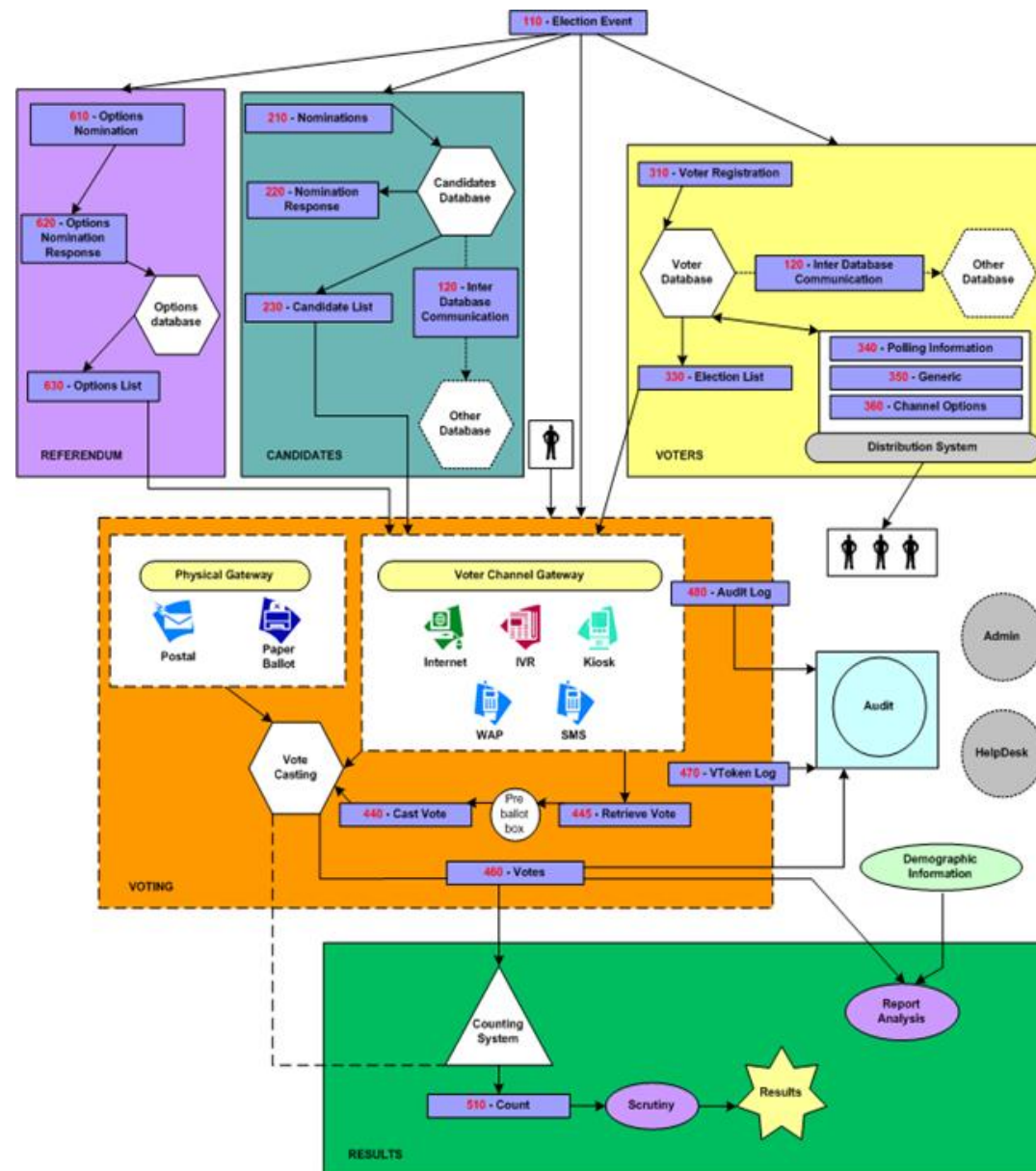
Requirements

- Multinational
adopted as international standards
- Flexible
effective across different voting regimes and voting channels
- Multilingual
accommodates various languages, dialects, vocabularies
- Adaptable
supports election in the private and public sectors
- Secure
secures the relevant data and interfaces from corruption

Benefits

- Trustworthiness of voting systems
- Security of the vote
- No proprietary lock-in
- Stability or reduction in costs
- Common core but customizable
- Basis for accreditation

High-Level Process Model (1)



High-Level Process Model (2)

Pre Election

- Election declaration
- Candidate nomination
- Referendum options
- Voter registration

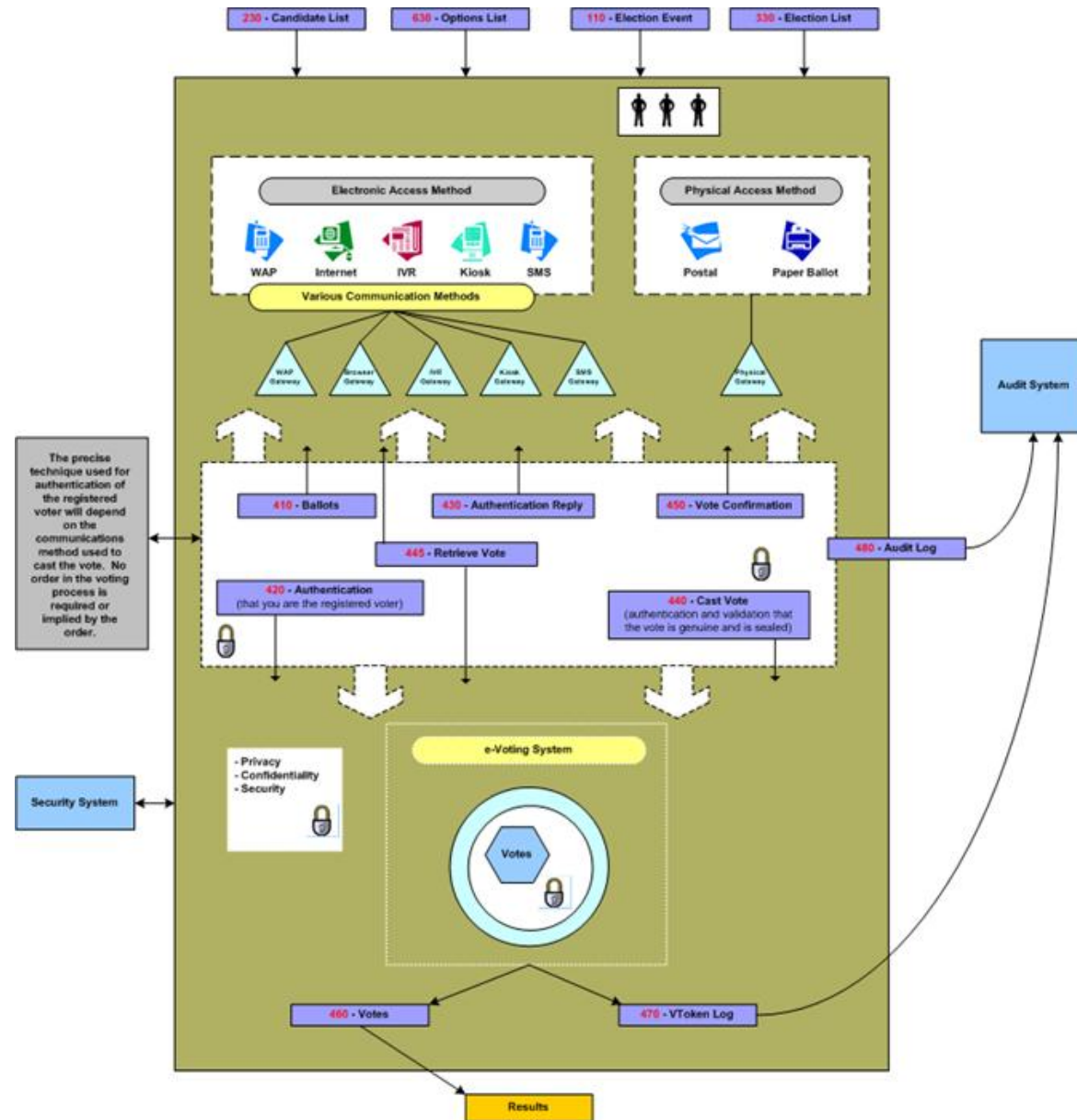
Election

- Ballot information
- Voter authentication
- Vote casting and confirmation

Post Election

- Election counts and results
- Audit

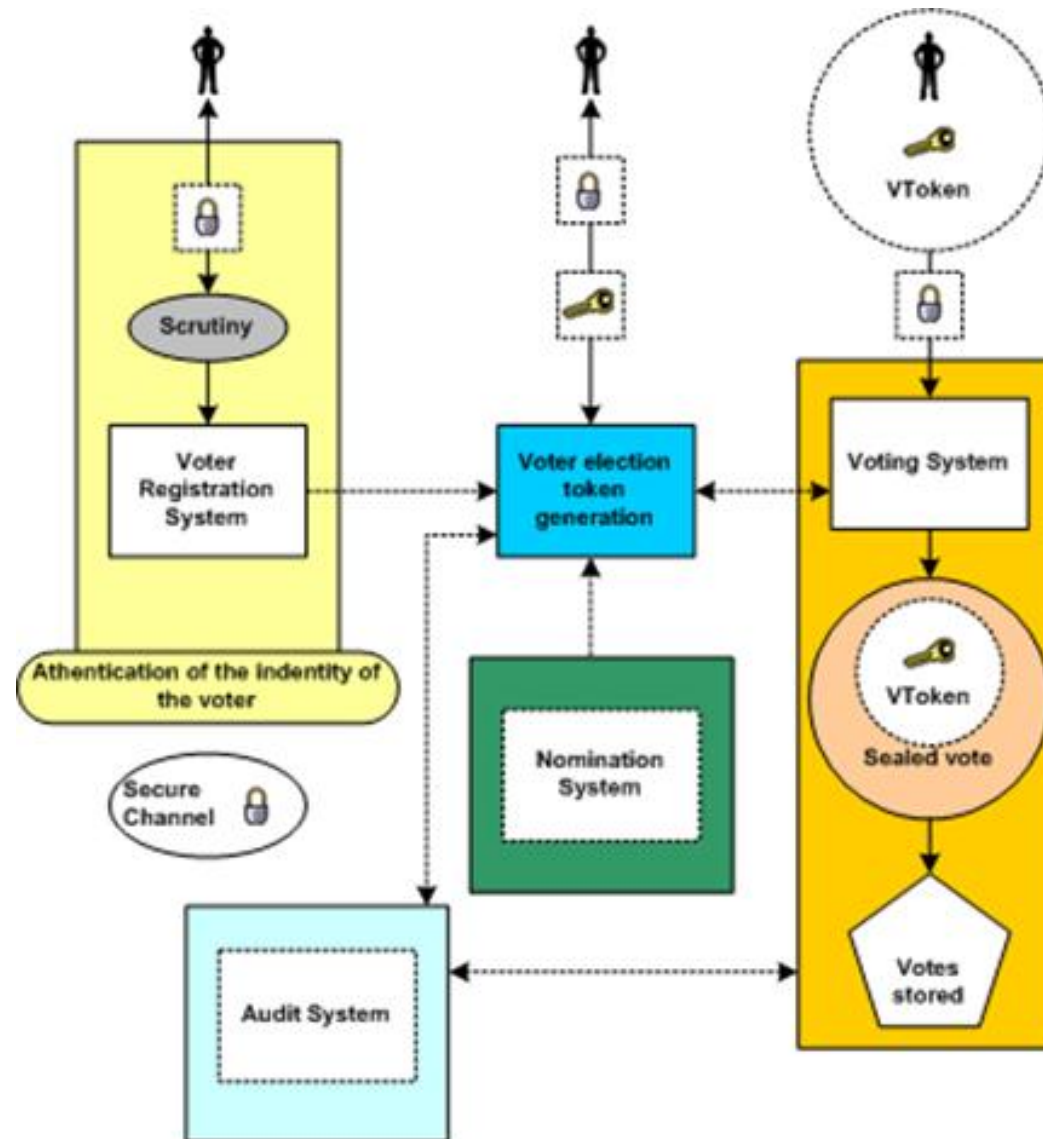
Voting Process



Security Requirements

- Only legitimate voters are allowed to vote
- Only one set of choices is allowed per voter, per contest
- The vote cannot be altered from the voter's intention
- The vote may not be observed until the proper time
- The voting system must be accountable and auditable
- Information used to authenticate the voter or his right to vote should be protected against misuse
- Voter privacy must be maintained according to the laws of the election jurisdiction
- The casting options available to the voter must be genuine
- Proof that all genuine votes have been accurately counted

Security Architecture (1)



Security Architecture (2)

- Voter identification and registration
- Right to vote authentication (VToken)
- Protecting exchange with remote voters
- Validation and contest vote (Seals)
- Vote confidentiality
- Candidate list integrity
- Vote counting accuracy
- Voting system security

References

- Cover Pages: Election Markup Language
<http://xml.coverpages.org/eml.html>
- OASIS Election and Voter Services TC
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=election
- Election Markup Language (EML) 5.0 Specification
<http://www.oasis-open.org/specs/index.php#eml5.0>
- Council of Europe, e-voting
<http://www.bmeia.gv.at/index.php?id=70339>
- The Co-ordinated Online Register of Electors (CORE)
http://www.dca.gov.uk/consult/core/core_cp2905.pdf
- IEEE Voting Systems Electronic Data Interchange
<http://grouper.ieee.org/groups/scc38/1622/>
- Open Voting Consortium
<http://www.openvotingconsortium.org/>
- Trusted Logic Voting Systems with OASIS EML 4.0
<http://drw.net/backup/Trusted-Logic-Voting-Systems-with-EML40.pdf>