E-vote 2011

Use case specification: 3.4 Counting of e-votes

Project: E-vote 2011

NORWEGIAN MINISTRY OF LOCAL GOVERNMENT AND REGIONAL DEVELOPMENT

CONTENT

1. Executive Summary

The system shall facilitate the secure and verifiable counting of e-votes, while safeguarding the principles of one voter/one vote maintaining the secrecy and anonymity of the vote. The system must have functionality for the counting valid e-votes maintaining the rules that:

a. P-votes overrides any e-votes
b. E-vote cast in a controlled environment overrides any e-votes later cast in an uncontrolled environment

2. Purpose

The purpose of this use case is to ensure that the votes are not manipulated and are counted in a secure environment.

3. Actors

Actor	Description
AI	Authorised individual

4. Pre-conditions

ID	Description	Comments
3.4.1	E-votes have been submitted	

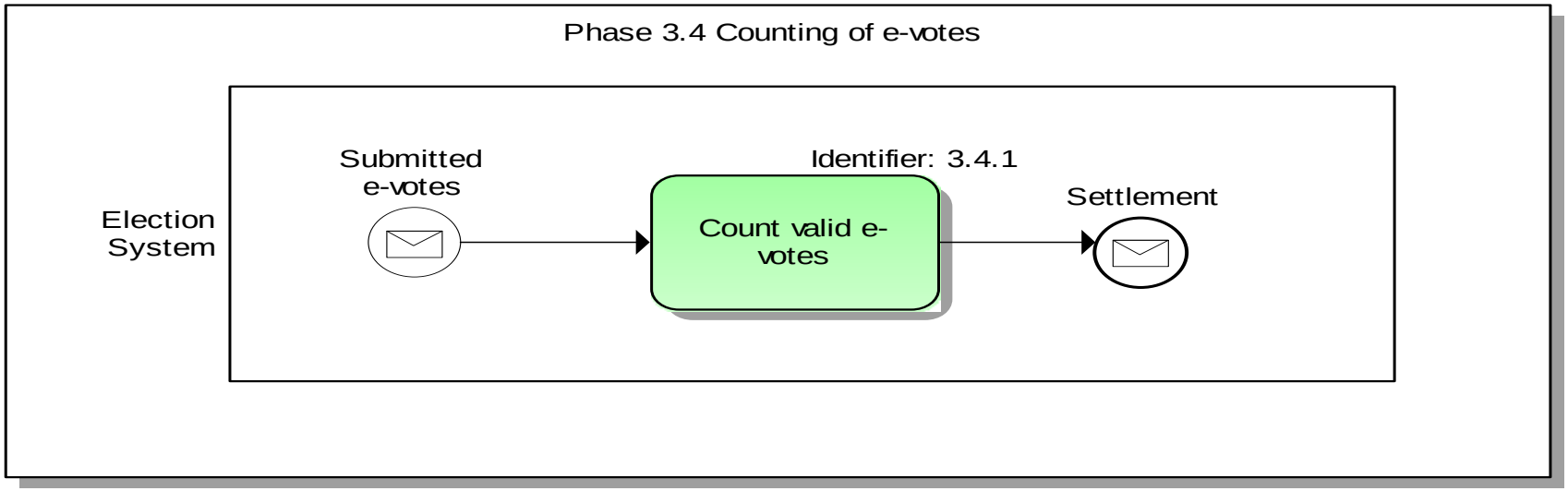
5. Post-conditions

ID	Description	Comments
3.4.3	E-vote totals are available in the system	The use case forms the basis for use case 4.2. ‘Settlement’

6. Trigger

There is a need for counting e-votes.

7. Main Flow - Functional Requirements



ID	Actor	Function (Requirement)	Requirement description	Ref
F 3.4.1	AI	Count valid e-votes	The system must facilitate the counting of valid e-votes (Last e-vote submitted). The system must be able to check to see whether the voter has: 1. Also cast a p-vote. A p-vote overrides any e-votes submitted. 2. Cast an e-vote in a controlled environment. E-vote cast in a controlled environment overrides any e-votes later cast in an uncontrolled environment The system must ensure the secrecy of the e-vote in the counting phase. E.g. in small constituencies the e-votes shall be counted together with another constituency.	

8. Non-functional Requirements

8.1. Accessibility and usability

ID	Requirement description	Ref 8.1
3.4.4	See 'Accessibility and usability requirements'	

8.2. Security

With regards to trust, this is a critical phase of an election, where the black box problem is at its most pronounced. Where counting and tabulation in p-voting is transparent and tangible, it is exactly the opposite in a computerized count of digital ballots. Making the source code available for experts to verification will not remove any shadow of doubt, as it is considered impossible to completely verify any non-trivial computer program. To further alleviate the black box problem, the report "Electronic voting – challenges and opportunities" suggests an N-version architecture. We do not intend to procure multiple versions of the election system, but we would like to explore the possibility of having a system architecture that will facilitate the parallel execution of several counting and tabulation-modules.

Note: N-version architectures require that N>2, and that versions are developed by different teams using different methodologies etc. Hence, what we are suggesting is not that the Tenderer use more than one instance of the same module to run in parallel. That would be pointless. What we are suggesting is *an architecture facilitating the parallel execution of independent modules performing the same tasks on the same input. This means that there is a requirement for clearly defined and open interfaces.*

ID	Requirement description
OS0.4	One and only one valid e-vote shall be counted per voter per contest
OS0.14	The election system shall not allow the disclosure of the number of votes cast for any voting option until after the end of the polling phase. This information shall not be disclosed to the public until after the end of the voting period.
OS3.3	The election system shall prevent processing information on votes cast within deliberately chosen sub-units that could reveal individual voters' choices.
OS3.4	The election system shall guarantee that votes when counted are, and will remain, anonymous, and that it is not possible to reconstruct a link between the vote and the voter.
OS8.12	The decryption of anonymous e-votes and the counting of e-votes shall be done in a part or parts of the election system that is not, and has never been, connected to any external network (air-gapped).
OS8.15	It shall be possible to manually verify the integrity of data transferred on removable media - or otherwise - between system modules

8.3. Rules & Regulations

ID	Requirement description
3.4.5	This use case refers to regulations described in the Representation of the People Act (RPA). http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/Regelverk/Representation_of_the_People_Act170609.pdf
3.4.6	This use case refers to regulations relating to parliamentary and local government elections (Representation of the People Regulations) http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/Regelverk/Regulations_2003_EN_170609.pdf
3.4.7	This use case also refer to the Council of Europe e-vote Recommendation Rec(2004) 11. http://www.coe.int/t/dgap/democracy/activities/GGIS/E-voting/Key_Documents/Rec(2004)11_Eng_Evoting_and_Expl_Memo_en.pdf

8.4. Performance (Frequency)

ID	Requirement description
P 3.4.1	The system must have capacity to count approximately 2 000 000 e-votes in 30 minutes.