E-Vote

August 14, 2012

1 Introduction

In this paper we descrived E-Vote a simple platform for online voting. Many online groups occasionally have the necessity of voting to elect a president, new members, or make collective decisions. These groups tend to have similar characteristics: members of the group communicate primarily via email (maling lists), members do not personally know each other and may not trust other members or managers of the group, members have various level of interest and engagement in the decisions of the community and are easily turned off by complex voting procedures.

We developed the E-Vote system to provide a service to these communities. The system has the following characteristics:

- The system is open source and anybody can check the source code. The code is small and written in the Python language. This makes it easy for professionals in the field to check it.

- The system can run as a service and one installation can run mutiple elections. Anybody can login into the system, create a new election, register voters and managers, and customize the ballot using an easy to use WYSIWYG interface.

- The system communicates with voters and managers by email.

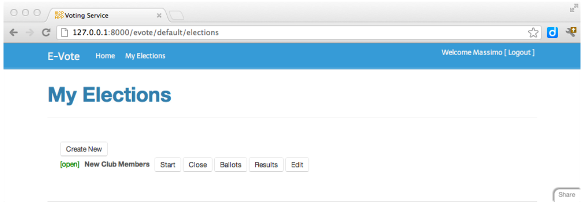
- Voters do not need to login into the system to vote. They only need to click on the link in the notification email, fill a web form and submit.

- Each voter can only vote once per election.

- Results are computed automatically at closing of the election and published.
- Voting is completely anonymous. Even a hacker with a complete database dump of the system would not be able to link voters to ballots.
- Each voter can check at any time that his vote has been properly recorded and not alatered.
- Each voter can independenty and at any time perform an election recount.
- Upon voting, each voter receives an email recipt containing a copy of their filled and anonymized ballot.
- Managers are notified by email when a new vote is cast and receive a copy of the anonimized ballot.
- All ballots, anonymized and digitally signed, are published, along with instruciton to verify the digital signature.

2 Workflow

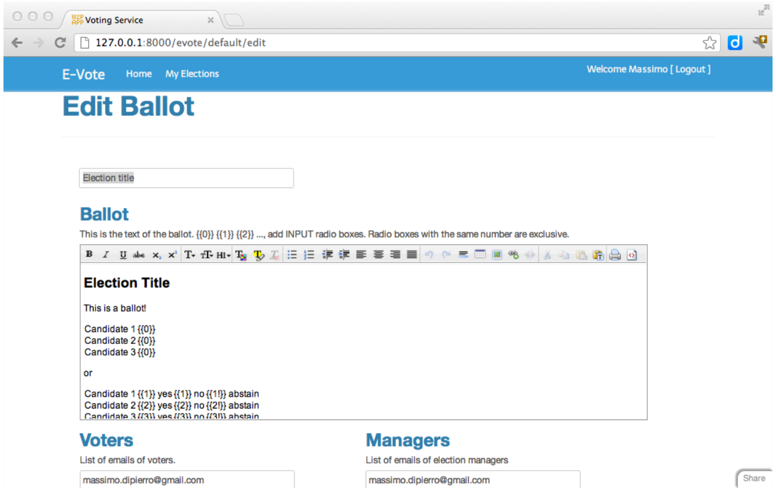
When a new user of the system wishes to create and run a new election, the user needs to login (voting does not require login, only managing an election requires login). We will refer to this user as the election officer.


Voting Service
127.0.0.1:8000/evote/default/elections
E-Vote
Home
My Elections
Welcome Massimo [Logout]

My Elections

[open] New Club Members

The election officer can create a new election by clicking on a button, editing the content of the model ballot, listing the emails of voters and those of the election managers, and declaring the election deadline. Election managers are users to be notified when a new vote is cast. The officer is also a manager.



Edit Ballot

Election title

Ballot

This is the text of the ballot. {{0}} {{1}} {{2}} ..., add INPUT radio boxes. Radio boxes with the same number are exclusive.

Election Title

This is a ballot!

Candidate 1 {{0}}
Candidate 2 {{0}}
Candidate 3 {{0}}

or

Candidate 1 {{1}} yes {{1}} no {{1!}} abstain
Candidate 2 {{2}} yes {{2}} no {{2!}} abstain
Candidate 3 {{3}} yes {{3}} no {{3!}} abstain

Voters

List of emails of voters.

massimo.dipierro@gmail.com

Managers

List of emails of election managers

massimo.dipierro@gmail.com

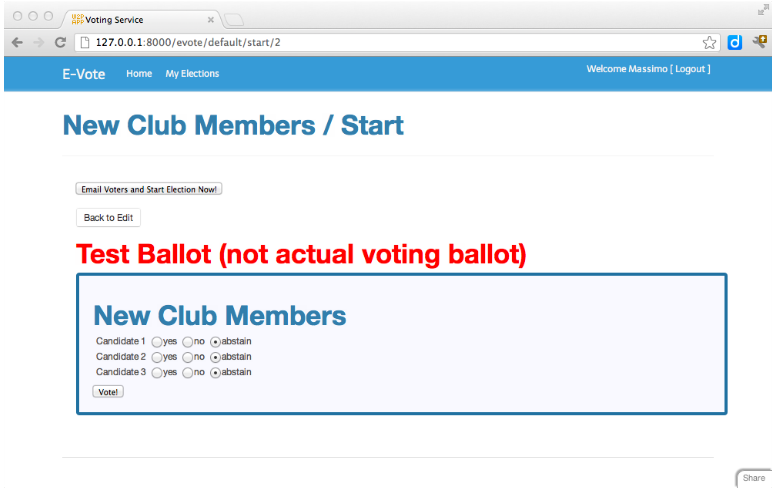
The model ballot is created using a WYSIWYG syntax similar to MS Word but using only the browsers. Special tags like {{0}} allow to insert radio boxes into the ballot. The voters will check these radio boxes. Two or more radio boxes identified by the same code belong to the same radio group and are exclusive. For example:

```
Do you agree? {{0}} yes or {{0}} no
```

Groups of radio boxes identified by different code are independent. For example:

```
Do you agree with A? {{0}} yes or {{0}} no
Do you agree with B? {{1}} yes or {{1}} no
```

After the election is created, it can be tested, and edited. New voters and managers can be added. Voters and managers do not have to be previous users of the system and do not need an account. The election starts by emailing memebrs:



Voting Service
127.0.0.1:8000/evote/default/start/2
E-Vote
Home
My Elections
Welcome Massimo [Logout]

New Club Members / Start

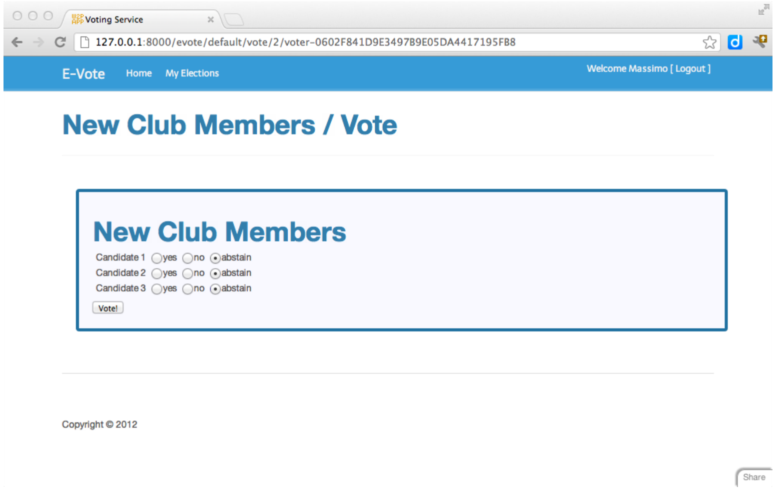
Email Voters and Start Election Now!
Back to Edit

Test Ballot (not actual voting ballot)

New Club Members

Candidate 1 ○ yes ○ no ● abstain
Candidate 2 ○ yes ○ no ● abstain
Candidate 3 ○ yes ○ no ● abstain

Each email listed by the officer corresponds to a voter. When the election starts a new record is created in the system for each voter. A voter record is uniquely identified by a voter-uuid code. UUID stands for a Universal Unique IDentifier. It is a long random sequence of characters that is impossible to guess. The voter-uuid is used to build a unique, one-time link, which is email to the voter and allow the user to vote.



Voting Service
127.0.0.1:8000/evote/default/vote/2/voter-0602F841D9E3497B9E05DA4417195FB8
E-Vote
Home
My Elections
Welcome Massimo [Logout]

New Club Members / Vote

New Club Members

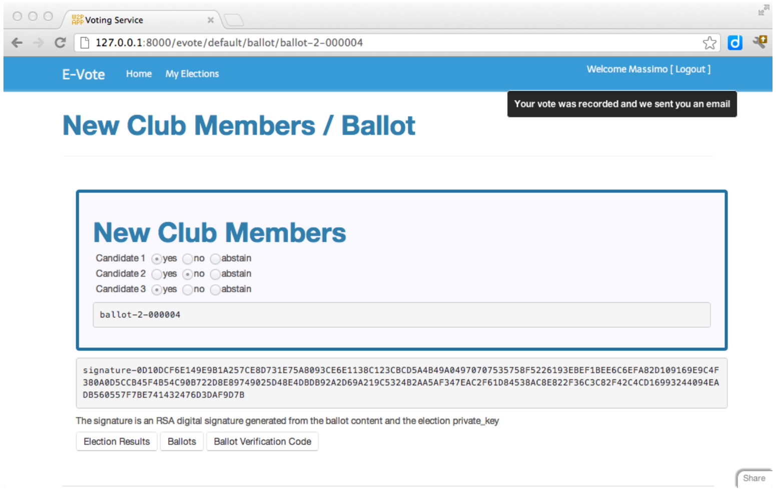
Candidate 1 ○ yes ○ no ● abstain
Candidate 2 ○ yes ○ no ● abstain
Candidate 3 ○ yes ○ no ● abstain

Copyright © 2012

The system recognizes the user from the voter-uuid in the URL.

When the election starts, the system also generates one ballot for each voter. A ballot is a BLANK form with a unique ID for the form ballot-in where id is comprised on an election id and a ballot id. Ballots are not linked to the voters at this time.

When a user fills and submits the voting form, the system picks a random ballot and records the vote on that ballot. The filled ballot, containing the vote and a unique `ballot-id`. The ballot is the digitally signed using the RSA algorithm using a private key associated to the election and only known to the system. The completed ballot, anonymized and signed, is published online, emailed to the user as a receipt, and emailed to the managers.



Voting Service
127.0.0.1:8000/evote/default/ballot/ballot-2-000004
E-Vote
Home
My Elections
Welcome Massimo [Logout]

Your vote was recorded and we sent you an email

New Club Members / Ballot

New Club Members

Candidate 1 ● yes ○ no ○ abstain
Candidate 2 ○ yes ● no ○ abstain
Candidate 3 ● yes ○ no ○ abstain

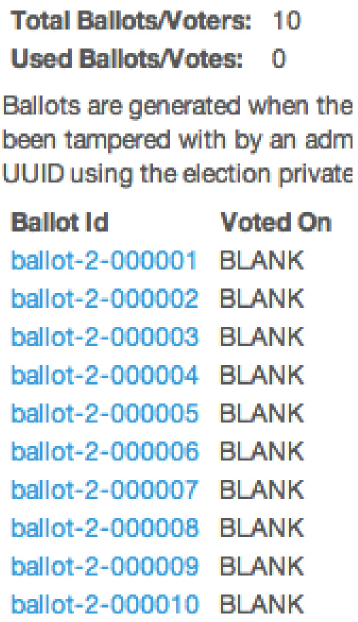
```
ballot-2-000004
```

```
signature-0D10DCF6E149E9B1A257CE8D731E75A8093CE6E1138C123CBCD5A4B49A04970707535758F5226193EBEF1BEE6C6EFA82D109169E9C4F
380A0D5CCB45F4B54C90B722D8E89749025D48E4DBDB92A2D69A219C5324B2AA5AF347EAC2F61D84538AC8E822F36C3C82F42C4CD16993244094EA
DB560557F7BE741432476D3DAF9D7B
```

The signature is an RSA digital signature generated from the ballot content and the election private_key

At this point the system has recorded that this voter has voted and its `voter-uuid` will no longer be useful for voting. The voter can check his vote was recorded because he received a receipt with a copy of the completed ballot.

When the election starts, the system also published a complete list of `ballot-id`. This allows everybody to check that new ballots have not been forged and some existing ballots have been used for voting.



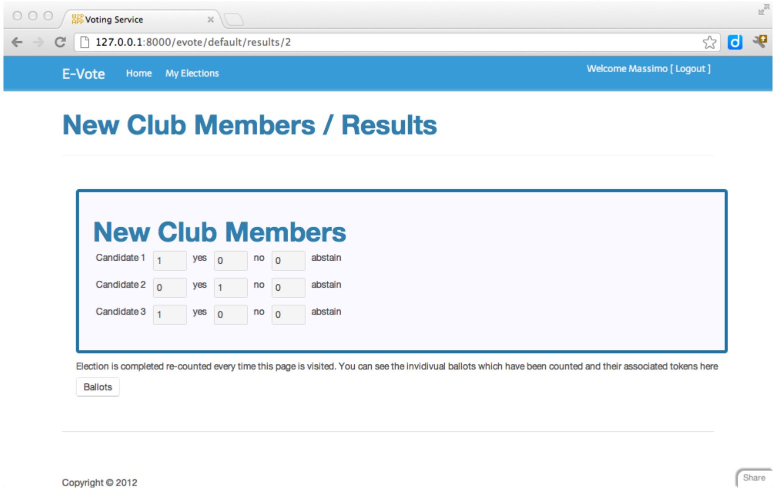
Total Ballots/Voters: 10

Used Ballots/Votes: 0

Ballots are generated when the
been tampered with by an adm
UUID using the election private

Ballot Id	Voted On
ballot-2-000001	BLANK
ballot-2-000002	BLANK
ballot-2-000003	BLANK
ballot-2-000004	BLANK
ballot-2-000005	BLANK
ballot-2-000006	BLANK
ballot-2-000007	BLANK
ballot-2-000008	BLANK
ballot-2-000009	BLANK
ballot-2-000010	BLANK

When the election is closed, results become public. The election is completely recounted evey time the `results` page is visited. The system counts how many times each checkbox has been clicked.


Voting Service
127.0.0.1:8000/evote/default/results/2
E-Vote
Home
My Elections
Welcome Massimo [Logout]
Share

New Club Members / Results

New Club Members

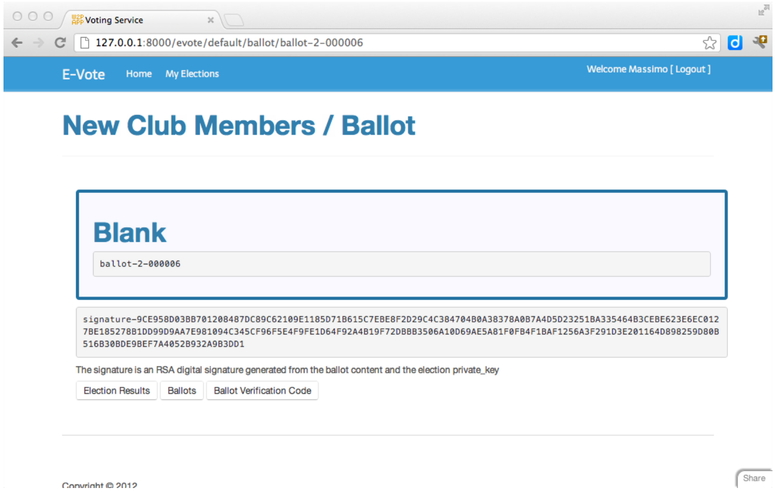
Candidate 1	1	yes	0	no	0	abstain
Candidate 2	0	yes	1	no	0	abstain
Candidate 3	1	yes	0	no	0	abstain

Election is completed re-counted every time this page is visited. You can see the invidivual ballots which have been counted and their associated tokens here

Ballots

Copyright © 2012

When the election closes some users may not have voted. They still need prof that their ballot is empty and has not been used by somebody else. For this purpose at closing of the election, the system emails every user who has not voted one of the remaining blank ballot as receipt.


Voting Service
127.0.0.1:8000/evote/default/ballot/ballot-2-000006
E-Vote
Home
My Elections
Welcome Massimo [Logout]

New Club Members / Ballot

Blank

ballot-2-000006

```
signature-9CE958D03BB701208487DC89C62109E1185D71B615C7EBE8F2D29C4C384704B0A38378A0B7A4D5D23251BA335464B3CEBE623E6EC012
7BE185278B1DD99D9AA7E981094C345CF96F5E4F9FE1D64F92A4B19F72DBBB3506A10D69AE5A81F0FB4F1BAF1256A3F291D3E201164D898259D80B
516B30BDE9BEF7A4052B932A9B3DD1
```

The signature is an RSA digital signature generated from the ballot content and the election private_key

In this way every user receive a receipt with a copy of their ballot (blank or filled).

```
https://127.0.0.1:8000/evote/default/elections
https://127.0.0.1:8000/evote/default/start/2
https://127.0.0.1:8000/evote/default/close_election/2
https://127.0.0.1:8000/evote/default/ballots/2
https://127.0.0.1:8000/evote/default/results/2
https://127.0.0.1:8000/evote/default/edit/2
https://127.0.0.1:8000/evote/default/vote/2/voter-160D...BE91
https://127.0.0.1:8000/evote/default/ballot/ballot-2-1
```

```
ballot-2-1
```

```
signature-5CF7...E246
```

```
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBAMTZTDA2xdl1DFisptWMVFdEt3gj+ROKrP3lYbntvJnPBzqf1/gmTqKb
rqzmQ+uSv6P5FIR1nuFX+17LBDjg0Ovz5bFYHxWYdRy4ObktUlvH+wOs0Byi7k0z
8ZAKIKJYJQgpZptS0rqxXRqREHmEyPKT5aE6oiL9AAEvKoVxuVmrAgMBAAE=
-----END RSA PUBLIC KEY-----
```

3 Validation Process

```
# import required libraries
import base64, rsa # install module with "pip install rsa".

# this is the ballot to verify
ballot = """
<div class="ballot"><h2>Election Title</h2>

<p>This is a ballot!</p>

<table>
<tbody><tr><td>Candidate 1</td><td><input disabled="disabled" name="ck_0" type="ra
<tr><td>Candidate 2</td><td><input checked="checked" disabled="disabled" name="ck_
<tr><td>Candidate 3</td><td><input disabled="disabled" name="ck_0" type="radio" va
</tbody></table>

<p>or</p>

<table>
<tbody><tr><td>Candidate 1</td><td><input checked="checked" disabled="disabled" na
<tr><td>Candidate 2</td><td><input checked="checked" disabled="disabled" name="ck_
<tr><td>Candidate 3</td><td><input checked="checked" disabled="disabled" name="ck_
</tbody></table><pre>
ballot-2-1
</pre></div>
""".strip()

# this is the ballot RSA signature
signature = base64.b16decode("5CF72361F326D5980C8B031DA8D7B4279AE29E592DD49633C732

# this is the election public key
pk_pem = """
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBAMTZTDA2xdl1DFisptWMVFdEt3gj+ROKrP3lYbntvJnPBzqf1/gmTqKb
rqzmQ+uSv6P5FIR1nuFX+17LBDjg0Ovz5bFYHxWYdRy4ObktUlvH+wOs0Byi7k0z
8ZAKIKJYJQgpZptS0rqxXRqREHmEyPKT5aE6oiL9AAEvKoVxuVmrAgMBAAE=
-----END RSA PUBLIC KEY-----
```

```
"""

# this is the code that verifies the signature
public_key = rsa.PublicKey.load_pkcs1(pk_pem)
if rsa.verify(ballot, signature, public_key)==None:
    print 'valid'
else:
    print 'invalid'
```

4 Conclusions

References

[1] ...