REVS - Installation and User Manual

22nd December 2004

1 Pre-requisites

To run REVS it is needed additional software, namely:

- MySQL version $\geq$ 3.23.53 MAX installed
  (available at http://www.mysql.com/)
- Java runtime version $\geq$ 1.4 installed
  (available at http://java.sun.com/)

Optional software

- OpenSSL (available at http://www.openssl.org/)

2 Key management

After the installation of the required software, the first step is to create and sign the keys of all servers (Commissioner, Ballot Distributors, Administrators, Anonymizers and Counters). To generate the keys we used the Java command line tool *keytool*.

2.1 Create a key

To create a key type the following command should be executed in the command line:

```
keytool -genkey -keystore kstore.ks -alias server -keyalg RSA -keysize 1024
-validity 365
```

This command creates a 1024 bits RSA key valid for 365 days. The key is stored in a keystore file named kstore.ks with the server alias. To find out more about keytool utility please check the Java documentation.

2.2 Sign a key

First we must create the signature request and submit it to a Certification Authority (CA) for signing. To create a signature request type the following command:

```
keytool -certreq -keystore kstore.ks -alias server -file server.req
```

This command will create a signature request for the key with the alias server and store it in the server.req file.

The second step is to get the certificate request signed. You can get your keys signed by a certification authority such as VerySign or you can create your own CA. We used the OpenSSL tool to create our own CA. After installing OpenSSL properly we use the following command to sign the request:

```
openssl x509 -req -in server.req -out server.crt -CA demoCA\cacert.crt -CAkey demoCA\private\cakey.crt -CAserial demoCA\serial
```

This command will use the CA installed in the *demoCA* directory to sign our request, the *cacert.crt* contains the CA public key certificate and the *cakey.crt* contains the CA private key. The signed request is stored in the *server.crt* file.

2.3 Import the signed certificate

Before importing the signed public key certificate we should first import the CA public key certificate.

```
keytool -import -file cacert.crt -keystore kstore.ks -alias ecca
```

This command imports the CA public key certificate *cacert.crt* to the keystore using the alias ecca (electoral commission certification authority). Then we can import our signed certificate:

```
keytool -import -file server.crt -keystore kstore.ks -alias server
```

Since the CA certificate is already in the keystore, it is possible to verify the signature on it and construct a valid certificate chain.

Note: use a different keystore file for each server.

3 Installing servers

3.1 Configuration file

For the Ballot Distributor, Administrator, Anonymizer and Counter servers there should be a configuration file defining the server and database addresses.

The configuration file is a text file that should look like this:

```
SERVER <address (//host/service_name)>
DATABASE <address (//host/database)>
```

Example:

```
SERVER //localhost/administrator
DATABASE //localhost/adm_database
```

3.2 Setting up servers

We have separated REVS in two jar files (*revs_servers.jar* and *revs_voter.jar*). For setting up the servers we use the revs_servers.jar file. To set up one REVS servers follow these steps:

1. Create the server's database in MySQL.
2. Copy the *revs_servers.jar* to the installation directory.
3. Create the subdirectories *"conf"* and *"ext"*.
4. Copy to the *"conf"* subdirectory the following files:
   (a) *kstore.ks* file: containing the key of the server, the signed public key certificate by the CA and the CA public key certificate (cf. Section 2).
   (b) *tstore.ks* file: containing the CA public key certificate (only for Anonymizers and Counters).
   (c) *commissioner.crt* file: The commissioner public key certificate signed by the CA.
   (d) *server.cfg* file: the server configuration file (cf. Section 3.1).
   (e) *policy.txt*: this file is a Java policy file; for more information about it consult the Java documentation. An example of a policy file is available at REVS download site.
5. Copy to the *"ext"* subdirectory the following files:
   (a) *soap.jar*: available at REVS download site.
   (b) *mysql-connector-java.jar*: available at REVS download site and at MySQL site.

Now we are ready to start the server. To start a Ballot Distributor, Administrator, Anonymizer or Counter server just type the following command:

```
    java -classpath "revs_server.jar;ext/soap.jar;ext/mysql-connector-java.jar;"
-Djava.security.policy=conf/policy.txt -Djava.rmi.server.codebase=file:/<full_directory_path>/revs_servers.j
inescID.revs.servers.StartServer
```

If everything is ok it should appear a menu to choose the server's type:

```
Select server type
0 - Distributor
1 - Administrator
```

```
2 - Anonymizer
3 - Counter
Server type:
```

After selecting the server's type it will be asked for the passwords for the database authentication, the keystore and the private key:

```
Press Enter for defaults.
user: REVSuser
password:REVSpassDB
KeyStore
password: REVSpassKS
Private key
password: REVSpassPK
```

The default values are only for the database authentication (user: sa, password: <*no_password*>). Finally, there should appear a list of actions allowed by the selected server:

```
K - Create signing keys (only Administrator)
F - Forward Counter selection (only Anonymizer)
G - Gather votes (only Counter)
T - Tally votes (only Counter)
C - Create database
D - Delete database
R - Redo database
U - Update database
S - Start server
E - Exit
Option:
```

To start the Commissioner server type the following command:

```
java -classpath "revs_servers.jar;ext\mysql-connector-java.jar;" -Djava.security.policy=conf/policy.txt
inescID.revs.commissioner.Commissioner
```

First it will be asked for the authentication information:

```
Press Enter for defaults.
user: REVSuser
password:REVSpassDB
KeyStore
password: REVSpassKS
Private key
password: REVSpassPK
```

And then the actions menu should appear:

```
C - Create tables
D - Delete tables
R - Redo tables
```

F - Fill tables
G - Graphic mode
E - Exit
Option:

All servers have three database management actions: create, delete and redo. **Before we can start using a server for the first time we must create the database tables.**

The remaining actions of each server will be explained in the next Sections.

4 Setting up an election

In REVS the election is prepared by using the *Commissioner* server. To set up an election start the *Commissioner* server as described in Section 3.2; if it is the first time do not forget to create the database tables. Then choose the option *G* to enter the graphic mode (see Figure 1), alternatively you can start the *Commissioner* server with the -*G* option (add -*G* at the end of the command to start the server). Now just follow these three steps:

1. First it is necessary to register the voters, option *Voters* in the *Commissioner* main menu (Figure 1). In the *Voter Administration* menu it is possible to add, remove or change the voters' records (Figure 2). When defining the passwords of the voters there are two options: a password and a pin or only one password (cf. Figure 3). In the case of using only one password the system internally splits it into two pieces, a "password" and a pin, to be used in the authentication algorithm defined in Section **??**.
   The voters are organized in groups and each voter can belong to several groups. To manage the groups of voters choose the option *Voters Groups* in the *Voter Administration* menu. In the *Group Administration* menu (Figure 4) it is possible to add and remove groups, to rename the group and to manage the voters in the groups (Figure 5). Note that the election electorate will be a voters' group.

2. The second step is to define an election configuration, option *Configurations* in the main menu. To define an election configuration it is necessary to define the polling period (start and end dates), the number of *Administrators* to use, the required signatures to make a vote valid and if *Anonymizers* are to be used. The *Configuration Administration* menu is shown in Figure 6.

3. To finish the election setups select the option *Elections* in the main menu. In the *Election Administration* menu (Figure 7) it is possible to create, delete or edit elections. To define an election it is necessary to define the name of the election, the election's ballot (cf. Section 4.1), the election's electorate (a voters' group) and the election's configuration. Note that

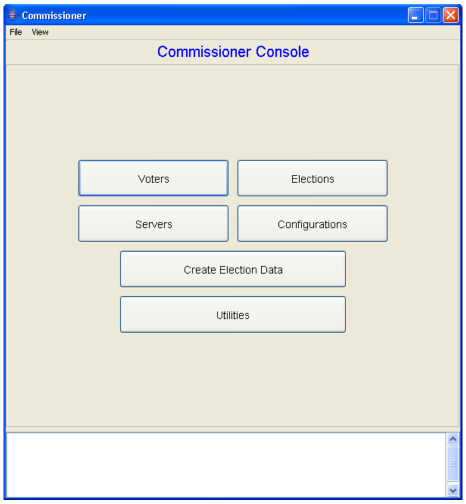


Figure 1: Commissioner main menu

several elections can use the same voters' group and/or election configuration.

4.1 Create a ballot

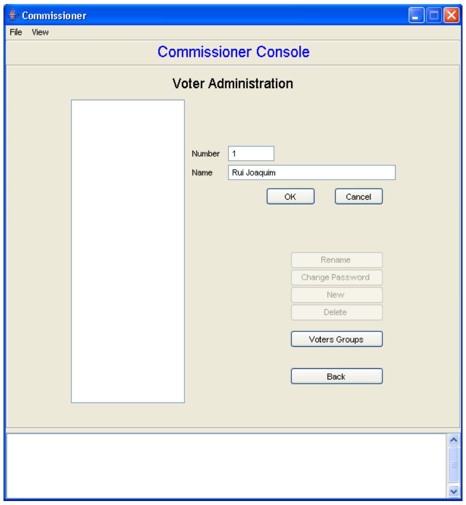
The ballots are defined in XML as presented in Figure 8. A ballot is composed by a description and several groups of questions. A group of questions has a description and several questions. A question is composed by a description, the question it self, and by the possible answers.

Currently four types of questions are supported: Single, the answer must be one and only one of the presented choices; Multiple, we can choose any number of choices for our answer; OpenS (open single) and OpenM (open multiple) types are similar to the Single and Multiple types respectively, but it is also possible to give another answer.

Currently there is no specific ballot editor. Therefore, it is necessary to use a text editor to create the election ballot.

4.2 Defining the election servers

Part of the setting up of REVS consists in defining the election servers, option *Servers* in the main menu. In the *Servers Administration* menu (Figure 9) it is possible to define the address and import the public key of the elections servers (Ballot Distributors, Administrators, Anonymizers and Counters). To import the public key of the server load the public key certificate file (cf. Section 2). Only the servers that are enabled can be used in the election.



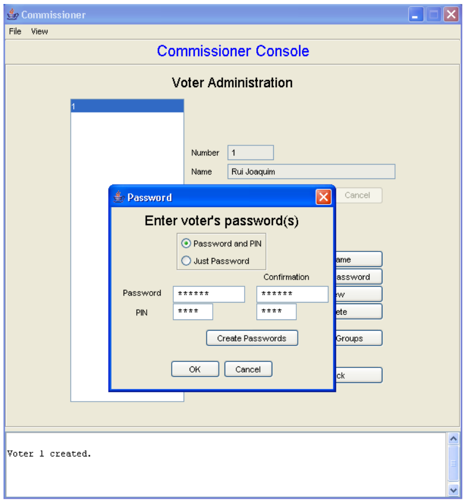
Commissioner Console

Voter Administration

Number 1

Name Rui Joaquim

Figure 2: Voters Administration menu



Commissioner Console

Voter Administration

Number 1

Name Rui Joaquim

Enter voter's password(s)

● Password and PIN
○ Just Password

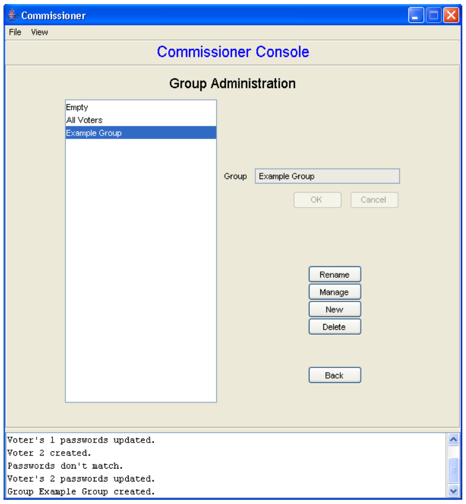
Confirmation

Password ****** ******

PIN **** ****

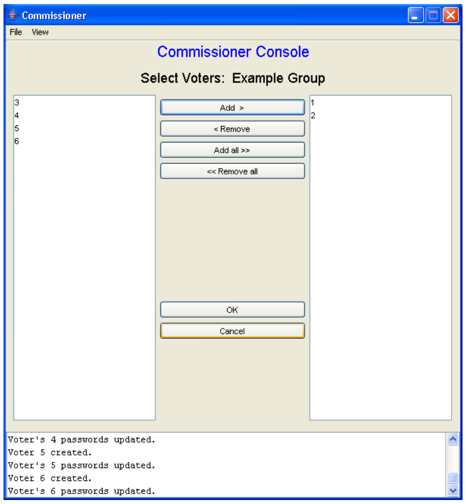
```
Voter 1 created.
```

Figure 3: Password menu



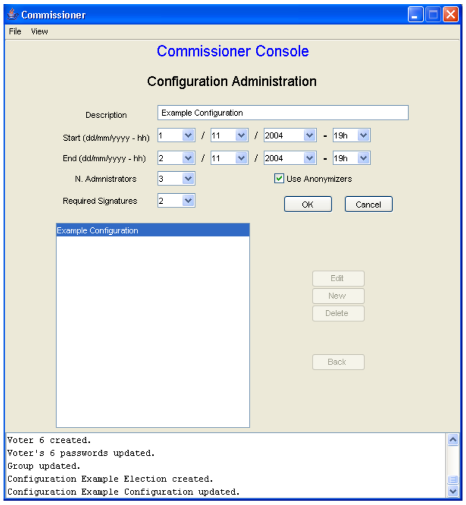
```
Voter's 1 passwords updated.
Voter 2 created.
Passwords don't match.
Voter's 2 passwords updated.
Group Example Group created.
```

Figure 4: Group Administration menu



```
Voter's 4 passwords updated.
Voter 5 created.
Voter's 5 passwords updated.
Voter 6 created.
Voter's 6 passwords updated.
```

Figure 5: Group management menu



Commissioner Console

Configuration Administration

Description: Example Configuration

Start (dd/mm/yyyy - hh): 1 / 11 / 2004 - 19h

End (dd/mm/yyyy - hh): 2 / 11 / 2004 - 19h

N. Administrators: 3

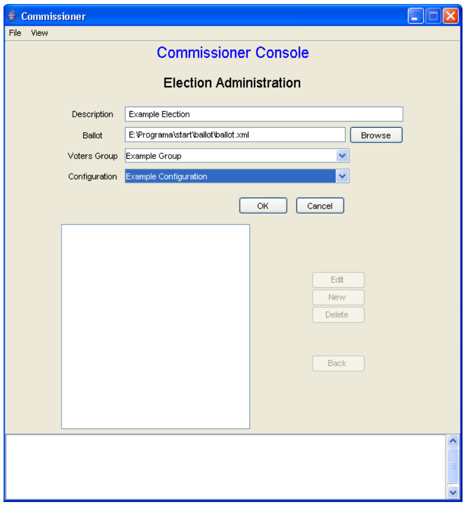
☑ Use Anonymizers

Required Signatures: 2

Example Configuration

```
Voter 6 created.
Voter's 6 passwords updated.
Group updated.
Configuration Example Election created.
Configuration Example Configuration updated.
```

Figure 6: Configuration Administration menu



Commissioner Console

Election Administration

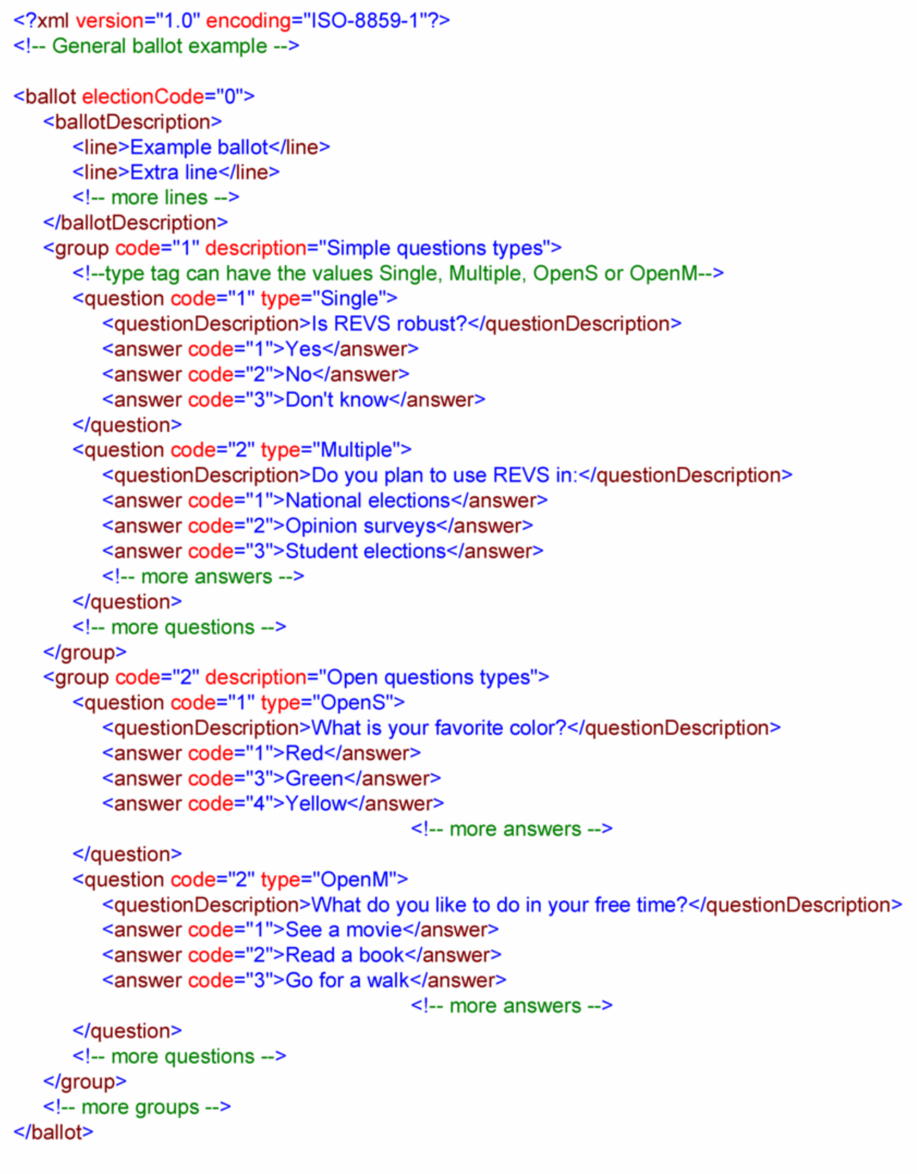
Description: Example Election

Ballot: E:\Programa\start\ballot\ballot.xml

Voters Group: Example Group

Configuration: Example Configuration

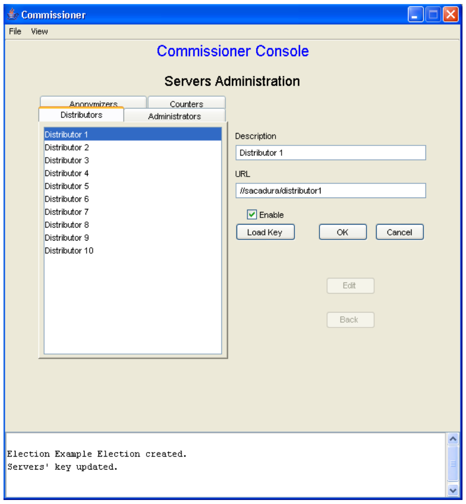
Figure 7: Election Administration menu



```xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<!-- General ballot example -->

<ballot electionCode="0">
    <ballotDescription>
        <line>Example ballot</line>
        <line>Extra line</line>
        <!-- more lines -->
    </ballotDescription>
    <group code="1" description="Simple questions types">
        <!--type tag can have the values Single, Multiple, OpenS or OpenM-->
        <question code="1" type="Single">
            <questionDescription>Is REVS robust?</questionDescription>
            <answer code="1">Yes</answer>
            <answer code="2">No</answer>
            <answer code="3">Don't know</answer>
        </question>
        <question code="2" type="Multiple">
            <questionDescription>Do you plan to use REVS in:</questionDescription>
            <answer code="1">National elections</answer>
            <answer code="2">Opinion surveys</answer>
            <answer code="3">Student elections</answer>
            <!-- more answers -->
        </question>
        <!-- more questions -->
    </group>
    <group code="2" description="Open questions types">
        <question code="1" type="OpenS">
            <questionDescription>What is your favorite color?</questionDescription>
            <answer code="1">Red</answer>
            <answer code="3">Green</answer>
            <answer code="4">Yellow</answer>
                                                    <!-- more answers -->
        </question>
        <question code="2" type="OpenM">
            <questionDescription>What do you like to do in your free time?</questionDescription>
            <answer code="1">See a movie</answer>
            <answer code="2">Read a book</answer>
            <answer code="3">Go for a walk</answer>
                                                    <!-- more answers -->
        </question>
        <!-- more questions -->
    </group>
    <!-- more groups -->
</ballot>
```

Figure 8: XML ballot



Description: Distributor 1

URL: //sacadura/distributor1

☑ Enable

```
Election Example Election created.
Servers' key updated.
```

Figure 9: Servers Administration menu

4.3 Import voters and elections

It is possible to import voters and elections from text files, using the appropriate commands at the *Utilities* menu, cf. Figure 10. The text files should have the following format:

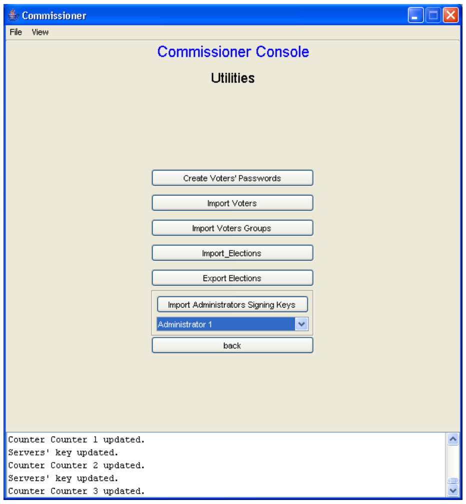
- Voters file (one line per voter):
  <id>;<name>[;password[;pin]]
  If the voters have no password information, use the option *Create Voters' Passwords* in the *Utilities* menu to create them.

- Voters' groups (one line per association group->voter):
  (<group id>|<group description>);<id_ voter>

- Elections file (one line per election):
  [<election id>;]<election description>;(<voters group id>|<voters group description>);<election configuration description>;<ballot file>
  Note that the election configuration must be created previously to the import of the elections file.

5 Start an election

To start an election it is necessary to create the servers' databases, option *Create Election Data* in the main menu of the *Commissioner*. The databases are created based on an election configuration instead of based on individual elections. Therefore, the databases created contain information concerning all the elections that have the selected configuration. In the *Configuration Selection*



```
Counter Counter 1 updated.
Servers' key updated.
Counter Counter 2 updated.
Servers' key updated.
Counter Counter 3 updated.
```

Figure 10: Utilities menu

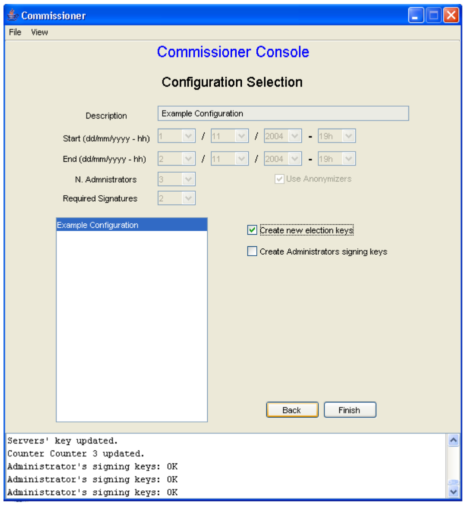
menu, cf. Figure 11, it is possible to select the election configuration and if it is necessary to create the elections' keys and/or the *Administrators* signing keys. If the keys are not in the *Commissioner* database an error message will appear. For security reasons the administrators signing keys should be created by the *Administrators* and not by the *Commissioner*, cf. Section 5.1.

After selecting the configuration press the *Finish* button to create the data files. The following files will be created:

1. One encrypted file containing the elections' private keys.
2. One file containing the decryption key to decipher the elections' private keys file.
3. One file for each enabled *Administrator*.
4. One file for the *Ballot Distributors*.
5. One file for the *Anonymizers* and *Counters*.
6. One file containing a list of the active *Ballot Distributors*.
7. One file containing a list of the active *Counters*.

All files are signed by the *Commissioner*.

The next step is to setup the servers' databases whith the created files. To load the files into a server's database, launch the server, cf. Section 3.2, select the *U - Update database* option and enter the file name. Now the server is ready to be started, just select the option *S - Start server*.



Commissioner Console

Configuration Selection

Description: Example Configuration

Start (dd/mm/yyyy - hh): 1 / 11 / 2004 - 19h

End (dd/mm/yyyy - hh): 2 / 11 / 2004 - 19h

N. Admnistrators: 3

☑ Use Anonymizers

Required Signatures: 2

Example Configuration

☑ Create new election keys

☐ Create Administrators signing keys

```
Servers' key updated.
Counter Counter 3 updated.
Administrator's signing keys: OK
Administrator's signing keys: OK
Administrator's signing keys: OK
```

Figure 11: Configuration Selection (create databases)

An additional step is required to start the *Anonymizer* server, it is necessary to select the *Counter* to which forward the votes. Select the option *F - Forward Counter selection* and enter the name of the file containing the list of active *Counters*, then select one. Now the server is ready to be started, just select the option *S - Start server*. It will be asked for the maximum number of ballots to be sent after each delay and the maximum delay time, cf. Section **??**.

5.1 Administrators signing keys

If the signing keys are created by the *Commissioner* is it possible for the *Commissioner* to keep the signing keys and use them produce valid votes, corrupting the election by it self. Therefore, is is recommended the creation of the signing keys by the *Administrators* and then import the verification keys to the *Commissioner*. The steps needed are the following:

1. Export the elections list to a file. Go to the *Utilities* menu and select the *Export Elections* option.

2. Create the signing keys for each *Administrator*. Start the *Administrator* server (cf. Section 3.2) and select the *K - Create signing keys* option. Then use the file saved in step one as input. The output is a file containing the signature verification keys.

3. Import the signature verification keys. In the *Utilities* menu and select the *Import Administrators Signing Keys* option.

6 Voting process

6.0.1 Start the *Voter's Module*

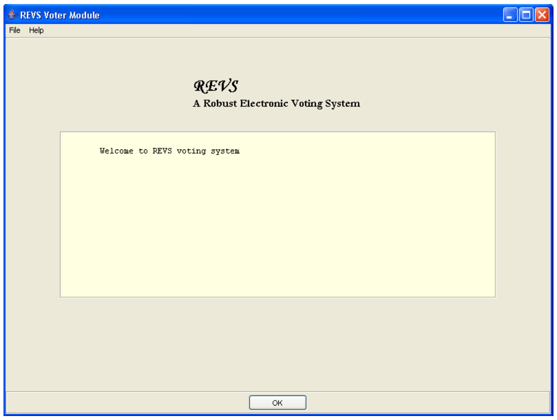
To install the *Voter's Module* copy the *revs_voter.jar* file to the installation directory and the following files to the *conf* subdirectory in the installation directory:

- *distributors*: the file containing the active Ballot Distributors list (cf. Section 5).
- *policy.txt*: this file is a Java policy file, for more information about it consult the Java documentation. An example of a policy file is available at REVS download site.
- *commissioner.crt*: this file contains the commissioner public key certificate signed by the CA.
- *tstore.ks*: this file contains the CA public key certificate. To create this file follow the instructions in cf. Section 2.3.
- *welcome.html*: this file contains the welcome message, formatted in HTML that appears on the welcome screen of the *Voter's Module* (Figure 12).

6.0.2 Voting steps

The voting steps are the following:

1. Start the *Voter's Module* with the following command:
   java -classpath "voter.jar" -Djava.security.policy=conf/policy.txt inescID.revs.voter.VoterEngine
   A welcome screen should appear (Figure 12). To continue press *OK*.
2. Then the voter authentication is requested (Figure 13). To continue press *OK*. A voter authentication confirmation should appear (Figure 14), to confirm press *Yes*.
3. The next screen presents the list of elections in which the voter can participate. The voter should pick one an press *OK* to continue (Figure 15).
4. Now it is displayed the ballot (Figure 16). The voter should fill in the ballot and when done press *OK* to submit the vote.
5. A validate confirmation message will appear (Figure 19). After the confirmation the vote is send to the Administrators for signing, but before that it is possible to save the voting state, cf. Figure 18, which is necessary to recover the voting process in the case of being impossible to submit the vote.



REVS
A Robust Electronic Voting System

Welcome to REVS voting system

Figure 12: Welcome screen

6. After collecting the administrators signatures it will appear a submit confirmation message (Figure 19). The vote is only submitted after this confirmation. If the voter does not confirm the submittion, the submittion is aborted. To resume the submit process it will be necessary the previously saved voting state.

7. Finally it is displayed the voting process report (Figure 20). From this menu it is possible to go to the election selection menu or to the welcome message menu.

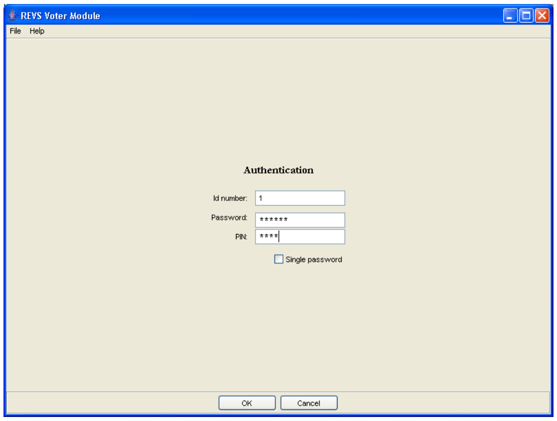
If the vote cannot be submitted successfully there will be an error message on voting process report. To resume the voting protocol go to the *File* menu, in the welcome screen, and select the *Resume Voting* option (Figure 21). Then the authentication menu should appear and the voting process is resumed.

7 Election tally

After the election polling close select the *Counter's* option *T - Tally votes* to decipher the votes, verify the *Administrators'* signatures and to produce the final election tally. For this action operation it will be needed the file containing the encrypted elections' private keys and the file containing the decryption key for the first one.

To view the results open the file *index.htm* in the *results* directory, a resume table of the elections results will appear (Figure). There it is possible to choose two views of the elections results (Figures and).

The *Counters'* option *G - Gather votes* should be used if there were multiple counters used in election to gather the voter from all of them. For this task it is necessary the file containing the list of active counters.



Authentication

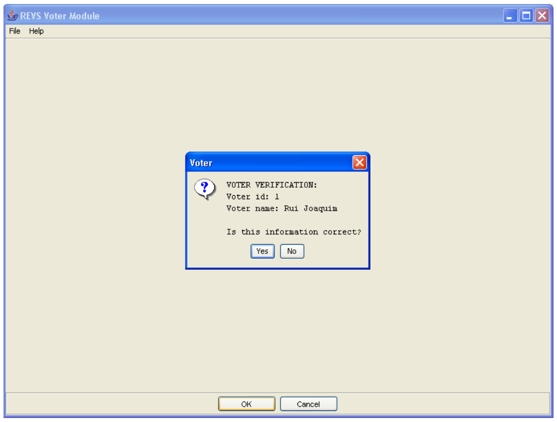
Id number: 1

Password: ******

PIN: ****

□ Single password

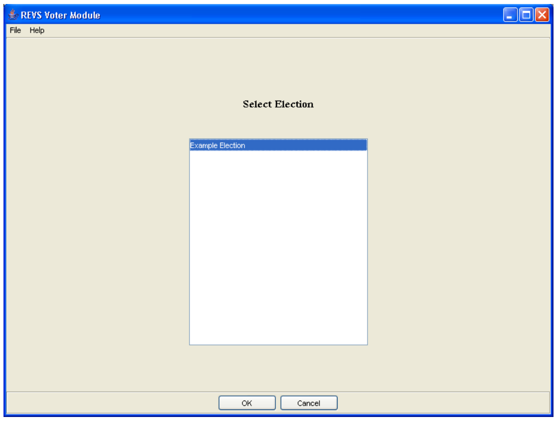
Figure 13: Authentication screen



```
VOTER VERIFICATION:
Voter id: 1
Voter name: Rui Joaquim

Is this information correct?
```

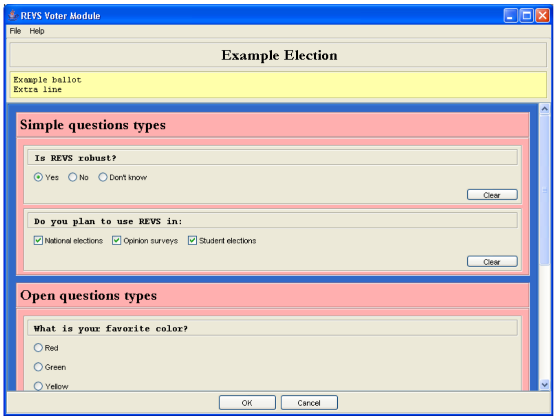
Figure 14: Authentication confirmation



Select Election

Example Election

Figure 15: Election selection screen



Example Election

```
Example ballot
Extra line
```

Simple questions types

Is REVS robust?

● Yes ○ No ○ Don't know

Do you plan to use REVS in:

☑ National elections ☑ Opinion surveys ☑ Student elections

Open questions types

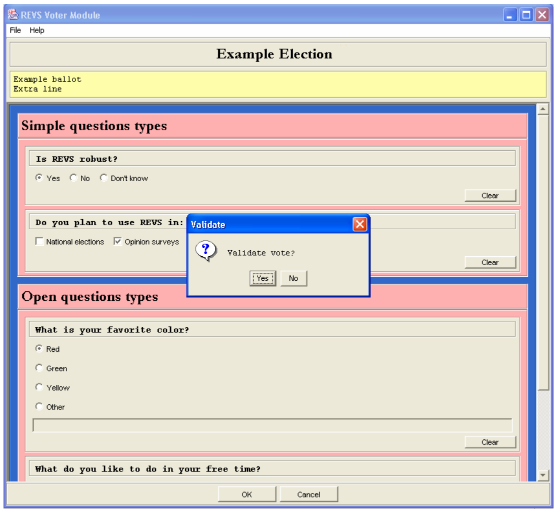
What is your favorite color?

○ Red

○ Green

○ Yellow

Figure 16: Ballot display



Example Election

Example ballot
Extra line

Simple questions types

Is REVS robust?

● Yes ○ No ○ Don't know

Do you plan to use REVS in:

□ National elections ☑ Opinion surveys

Validate

Validate vote?

Open questions types

What is your favorite color?

● Red

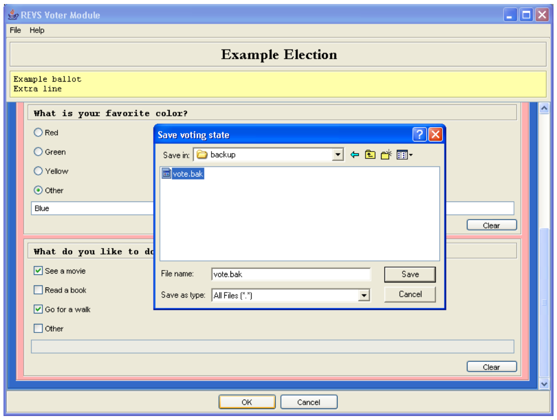
○ Green

○ Yellow

○ Other

What do you like to do in your free time?

Figure 17: Validate confirmation



Example Election

Example ballot
Extra line

What is your favorite color?

○ Red

○ Green

○ Yellow

● Other

Blue

Save voting state

Save in: backup

vote.bak

File name: vote.bak

Save as type: All Files (*.*)

What do you like to do

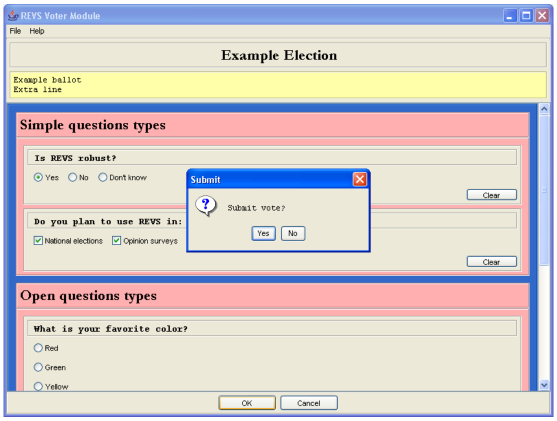
☑ See a movie

□ Read a book

☑ Go for a walk

□ Other

Figure 18: Save vote state



Example Election

Example ballot
Extra line

Simple questions types

Is REVS robust?

● Yes ○ No ○ Don't know

Do you plan to use REVS in:

☑ National elections ☑ Opinion surveys

Submit vote?

Open questions types

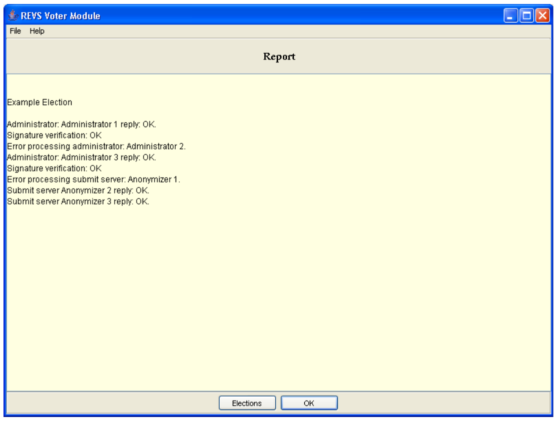
What is your favorite color?

○ Red

○ Green

○ Yellow

Figure 19: Submit confirmation

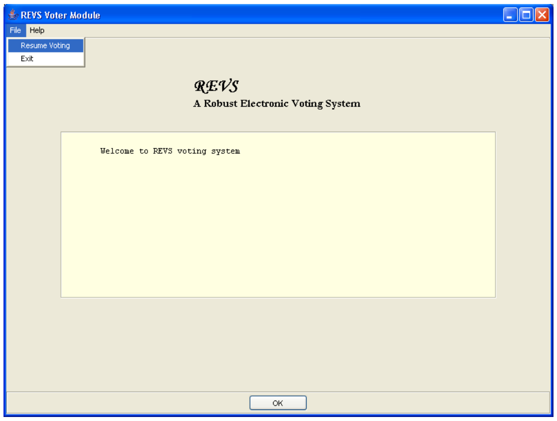


Report

```
Example Election

Administrator: Administrator 1 reply: OK.
Signature verification: OK
Error processing administrator: Administrator 2.
Administrator: Administrator 3 reply: OK.
Signature verification: OK
Error processing submit server: Anonymizer 1.
Submit server Anonymizer 2 reply: OK.
Submit server Anonymizer 3 reply: OK.
```

Figure 20: Report screen

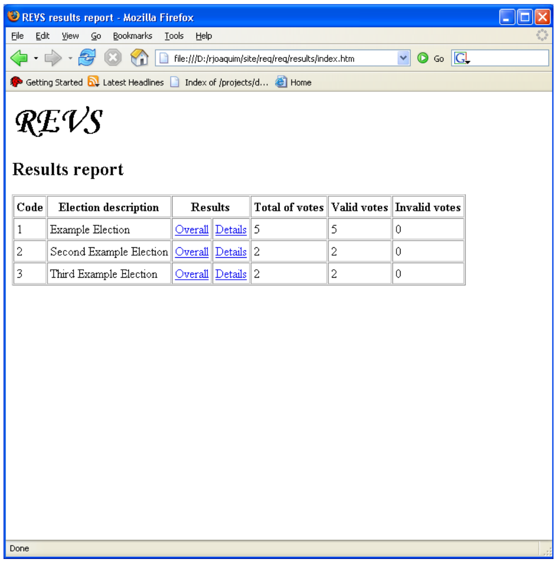


REVS

A Robust Electronic Voting System

```
Welcome to REVS voting system
```

Figure 21: Resume voting

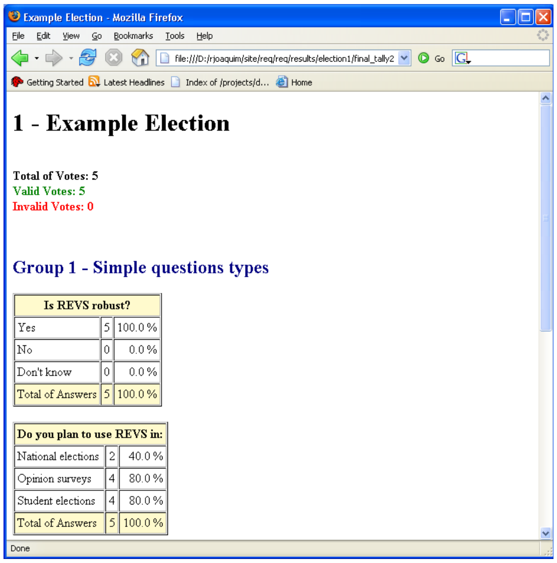

REVS results report - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
file:///D:/rjoaquim/site/req/req/results/index.htm
Go
Getting Started
Latest Headlines
Index of /projects/d...
Home
Done

REVS

Results report

Code	Election description	Results		Total of votes	Valid votes	Invalid votes
1	Example Election	Overall	Details	5	5	0
2	Second Example Election	Overall	Details	2	2	0
3	Third Example Election	Overall	Details	2	2	0

Figure 22: Results resume table


Example Election - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
file:///D:/rjoaquim/site/req/req/results/election1/final_tally2
Go
Getting Started
Latest Headlines
Index of /projects/d...
Home
Done

1 - Example Election

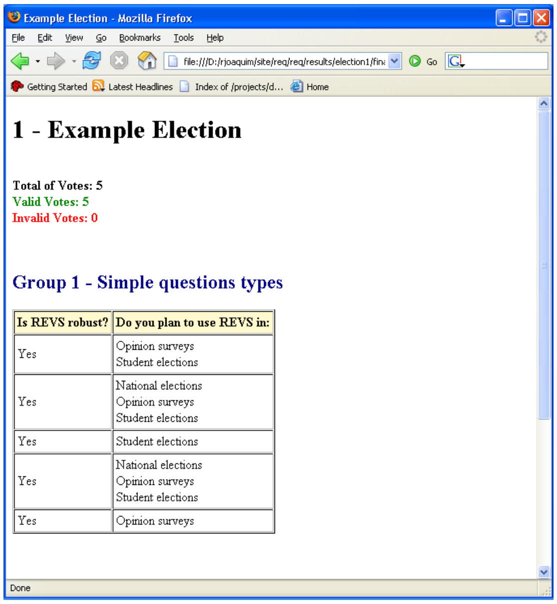
Total of Votes: 5
Valid Votes: 5
Invalid Votes: 0

Group 1 - Simple questions types

Is REVS robust?		
Yes	5	100.0 %
No	0	0.0 %
Don't know	0	0.0 %
Total of Answers	5	100.0 %

Do you plan to use REVS in:		
National elections	2	40.0 %
Opinion surveys	4	80.0 %
Student elections	4	80.0 %
Total of Answers	5	100.0 %

Figure 23: Overall results


Example Election - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
file:///D:/rjoaquim/site/req/req/results/election1/fina
Go
Getting Started
Latest Headlines
Index of /projects/d...
Home
Done

1 - Example Election

Total of Votes: 5
Valid Votes: 5
Invalid Votes: 0

Group 1 - Simple questions types

Is REVS robust?	Do you plan to use REVS in:
Yes	Opinion surveys Student elections
Yes	National elections Opinion surveys Student elections
Yes	Student elections
Yes	National elections Opinion surveys Student elections
Yes	Opinion surveys

Figure 24: Results details