USER MANUAL
Online Collection Software for European Citizens' Initiatives

1 General presentation

This software has been designed for organisers of European citizens' initiatives.

It has been developed by the European Commission and already complies with the functional, application and database related requirements of the technical specifications[1]. It provides all the necessary functionalities to collect statements of support online, securely store signatories' data and export the data to the competent national authorities. It can easily be configured for any proposed citizens' initiative as it enables organisers to upload all relevant information on their initiative from their organiser account on this website.

The software consists of a public interface for signatories to give their support and an administration interface for organisers to manage the system.

Both interfaces are available in all 23 official languages of the European Union.

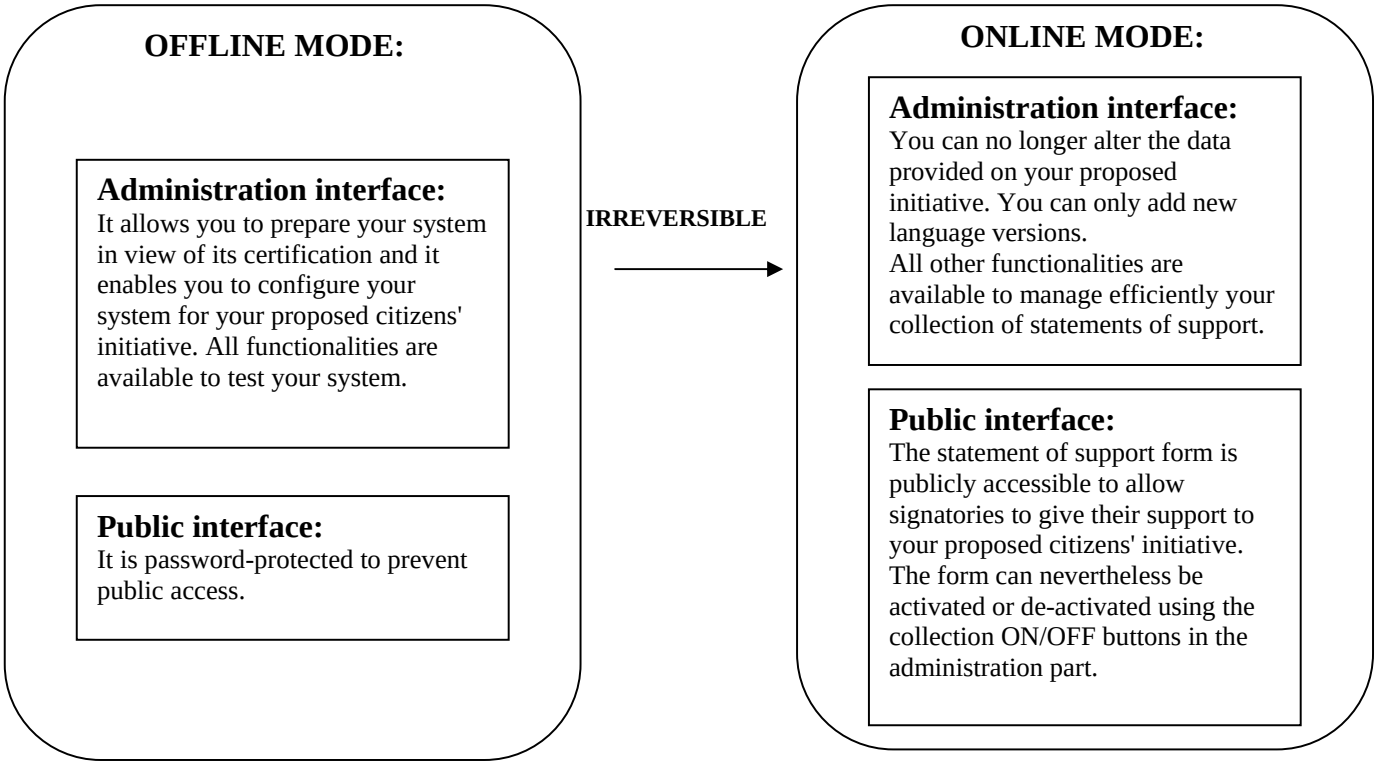
The software can be in two different modes:

- ***Offline mode***: this mode enables the organisers/administrators to prepare and test the system prior to starting the collection campaign. In this mode, the public interface is password protected to prevent access from the general public.
- ***Online mode***: this mode refers to the state of the system once it has been set up. This mode allows organisers to start collecting statements of support for their proposed citizens' initiative.

By default, the system is in offline mode. The transition to online mode is under the control of the organisers/administrators. In order to go into online mode, the organiser/administrator is required to finalise the set up of the system using the initiative data registered on the European Commission register for the Citizens' Initiative (hereafter 'ECI register') and to have uploaded the conformity certificate issued by the competent national authority. Transition to online mode has the effect of disabling the password protection of the public interface so that actual collection of statements of support can start.

Important: Transition from offline to online mode is irreversible!

[1] Commission Implementing Regulation (EU) No 1179/2011 of 17 November 2011 laying down technical specifications for online collection systems pursuant to Regulation (EU) No 211/2011 of the European Parliament and of the Council on the citizens' initiative


OFFLINE MODE:
Administration interface:
It allows you to prepare your system in view of its certification and it enables you to configure your system for your proposed citizens' initiative. All functionalities are available to test your system.
Public interface:
It is password-protected to prevent public access.
IRREVERSIBLE
ONLINE MODE:
Administration interface:
You can no longer alter the data provided on your proposed initiative. You can only add new language versions.
All other functionalities are available to manage efficiently your collection of statements of support.
Public interface:
The statement of support form is publicly accessible to allow signatories to give their support to your proposed citizens' initiative. The form can nevertheless be activated or de-activated using the collection ON/OFF buttons in the administration part.

2 Install the software in your system

2.1 Application database preparation

The Online Collection Software (OCS) uses a relational database for application configuration and collected data storage. The database engine is accessed by the Java Database Connectivity standard protocol.

OCS supports and provides scripts for the Oracle Database Engine and MySQL (see the following sections).

Please note that the SQL scripts containing schema definitions and application data do not contain any database creation statements - the **database must be created before executing the script**, using the native tools of the underlying engine.

OCS requires the database to use *UTF-8* as a character encoding.

2.1.1 Oracle Database 11g

To create the OCS database for Oracle, the script `oct-oracle-schema-create.sql` must be executed. It creates the database schema including tables, sequences and indexes, and populates the tables with initial data.

In order to drop the OCS database, the following script might be helpful: `oct-oracle-schema-drop.sql`

OCS supports Oracle Database 11g. Although the system might also work on previous versions of the Oracle Database engine, this has neither been tested, nor can it be supported by the supplier of the system.

2.1.2 *MySQL 5.5+*

To create the OCS database for MySQL, the script `oct-mysql-schema-create.sql` must be executed. It creates the database schema including tables, sequences and indexes, and populates the tables with initial data.

In order to drop the OCS database, the following script might be helpful: `oct-mysql-schema-drop.sql`

OCS supports MySQL 5.5 and greater. Although the system might also work on previous versions of the MySQL engine, this has neither been tested, nor can it be supported by the supplier of the system.

2.2 System initialisation

In order to configure the system, the application database must be populated with a small number of environment specific settings, which are described in the following parts of this section.

2.2.1 Application file storage

The application uses a server side file system to output application artefacts, such as exported collected data. The server side file storage should be capable of accommodating exported data packages up to a recommended capacity of 10 GB.

The **absolute path to the file system storage** on the application server must be inserted into the only row of the `OCT_SYSTEM_PREFS` table, column `FILE_STORE`.

The value can simply be inserted into the row that has been created by the database initialisation script, see section 2.1.

Please note that **only one row** is allowed in the `OCT_SYSTEM_PREFS` table.

2.2.2 Cryptography tool installation

The Cryptography tool is a standalone application responsible for decrypting collected data. It is also required for the web application authentication process, as it provides the functionality for decrypting the authentication challenge phrase which is asked in the login screen.

In order to install the application, a distribution archive needs to be unpacked into the file system. The Cryptography tool is a Java application and thus platform-independent. However the package provides operating system specific distributions, which contain a convenient launcher script for the underlying operating system. Only one of these distributions needs to be unpacked.

The shipped distributions support Windows or Linux and are named `oct-crypto-win32.zip` or `oct-crypto-linux.zip`, respectively. The launcher script is located in the `bin` directory and named either `launcher.bat` or `launcher.sh`, depending on the platform.

When the application is run for the first time, the only available menu option is *Initialize*. Upon selection, the application prompts the user to create a **master password**. This password will be used to protect both the private key within the Cryptography tool and the password for the web application administrator account. It will also be used to access the Cryptography tool once it is initialised.

After entering and submitting the password in the Cryptography tool, the user is presented a **public key** and a **hashed password** information. One folder is also created called **data** inside the cryptography tool installation folder. This folder contains three files:

- crypto.key – contains the encrypted private key
- oct.key – contains the public key in a hexa-decimal form (the same as the one presented in UI)
- crypto.salt – the file that is used for decrypting the private key

It falls within the responsibility of the administrator to not forget the password entered at this phase or delete/lose the data folder. These data are stored with a very strong encryption mechanism making it impossible to provide a password recovery or a password reset mechanism. As such it is mandatory for these files to be kept safely.

Note: The data folder is portable. As such, if you deleted by mistake the Cryptography tool but you have a back-up copy of the data folder, all you need to do is to reinstall the Cryptography tool and to copy in the installation folder the backed-up data folder. The Cryptography tool will recognise those data and consider the tool initialised with the password used when the original data folder was created.
The password used for initializing the Cryptography tool will be used to access the Cryptography tool once it is initialized.

2.2.2.1 *Public key to be inserted in the Online Collection Software prior to deployment.*

The Cryptography tool initialisation output window presents the newly generated public key within the text area labelled *Public key*.

The value in this text area must be inserted into the single row of the `OCT_SYSTEM_PREFS` table, column `PUBLICKEY`.

Note: One must pay attention to insert the value into the already existing row, as **only one row** is allowed in the `OCT_SYSTEM_PREFS` table.

2.2.2.2 *Web account login and password*

The second value presented on the Cryptography tool initialisation output window is the *Hashed password*.

This value is used for setting up the password of the initial administrator account in the web system. The account entries are stored in the database table `OCT_ACCOUNT`. The user must create a row for the initial account, where the USERNAME column value represents the account name (login), and the value for the PASSHASH column is the hashed password copied from the output window of the Cryptography tool. If later on the administrator password needs to change or if the admin would simply want to use a different password for accessing the online part than the password used to access the crypto tool, this can be done via the Password hashing functionality of the Cryptography tool. Please note that this functionality does not affect the password set for the Cryptography tool.
In order to obtain a new '*Hashed password*', start the Cryptography tool and navigate to the Menu -> Hash password. This will open a simple window with one input field for the desired value and when clicking on the 'hash password' button, the 'Hashed password' field will be filled up with the corresponding '*Hashed password*'.

2.3 Application deployment

The OCS application is fully compliant with Java Enterprise Edition (JEE) version 5. It can be hosted on any middleware software providing the following services: Enterprise Java Beans 3.0, Servlet 2.5, JMS and Java Persistence API 2.0.

The application requires JEE resources to be configured within the application server, which are discussed in detail in the following sections.

2.3.1 Configuration of JEE resources

The following list of resources needs to be created within the application server. For a system running on Oracle Weblogic Application Server or GlassFish, one can take advantage of the scripts provided alongside the application, which are discussed in the next subsections. Otherwise the required resources will have to be created manually.

2.3.1.1 Java Messaging System

The following Java Messaging System (JMS) items need to be created:

Item type	JNDI name
JMS connection factory	`OctExportQueueConnectionFactory`
JMS Queue	`OctExportQueue`
JMS Queue	`OctExportDispatcherQueue`

The JMS queues are being used for an asynchronous export feature. In order to optimise system performance, one should configure them for 20 threads.

Transaction support (XA) must be enabled for these resources.

2.3.1.2 Data Source

The following data source needs to be created:

Item type	JNDI name
Data Source	`jdbc/oct`

The data source must be set up with all required parameters for connecting to the database configured in section 2.1: Application database preparation. These include, in general, the name **and port of the database server**, the **name of the database**, as well as a **user name and password** for connecting to the database.

The data source must support transactions (XA).

Please note that the application server might also need a suitable JDBC driver to be installed, in order to connect to the selected database engine. Whether this is necessary or not depends on the actual combination of application server and database engine. Please refer to the technical manuals of these products, in order to determine if and how a JDBC driver needs to be installed, and where to obtain it.

2.3.1.3 Configuration on Oracle Weblogic Application Server 10.3.4+

Oracle Weblogic uses an API called WLST for administering system resources of the application server. WLST is implemented as a Python environment running on a Java platform. OCS provides a Python script which can be executed within the WLST engine, and which initialises all required JEE resources.

The name of the script is
`oct-weblogic-10.3.4.py`.

The procedure for creating a Weblogic server configuration is as follows:

- customise the Python script by providing valid values for the following variables describing the configuration of the Weblogic instance: `SERVER_HOST, SERVER_PORT, WL_ADMIN_USER, WL_ADMIN_PASS, WL_INSTANCE` and the underlying database engine: `DB_DIALECT, DB_HOST, DB_PORT, DB_NAME, DB_USER, DB_PASS`
- launch WLST by executing `WL_HOME/common/bin/wlst.cmd` or `.sh`
- execute the script within the WLST console:
  - `execfile('<PATH_TO_SCRIPT>')`
- exit the WLST console:
  - `exit()`

See also the Oracle Weblogic documentation for more information on WLST.

The supported Oracle Weblogic platform is 10.3.4 or later. The configuration script is not guaranteed to work on any previous version of the Oracle Weblogic application server.

2.3.1.4 Configuration on GlassFish OpenSource Edition 3

The GlassFish application server provides various ways of configuring JEE resources, one of which are XML configuration files which can be loaded by a server administration tool. This approach seems simple and convenient, and was therefore chosen for the OCS project.

OCS provides two separate XML configuration files for the initialisation of required JEE resources:

- oct-glassfish-3.1.1-mysql.xml
- oct-glassfish-3.1.1-oracle.xml

1. For a database engine among the ones above, the corresponding configuration file needs to be customised and loaded into the GlassFish server. The detailed configuration procedure is as follows: customise the selected XML file by replacing all placeholders (`$DB_USER, $DB_PASSWORD, $DB_HOST, $DB_PORT, $DB_NAME`) in the *** CUSTOMISE *** section of this file with the actual values
2. launch the GlassFish administration tool with the option to create resources based on the selected XML file:
   `GLASSFISH_HOME/bin/asadmin -H GLASSFISH_HOST -p GLASSFISH_PORT -u GLASSFISH_ADMIN_USER add-resources <PATH_TO_XML_FILE>`
   - where:`GLASSFISH_HOME` – GlassFish installation directory,
   - `GLASSFISH_HOST` – GlassFish host name (usually localhost),
   - `GLASSFISH_PORT` – GlassFish port number,

- `GLASSFISH_ADMIN_USER` – GlassFish administrator account name

The supported GlassFish platform is 3.1.1 or later. The configuration files are not guaranteed to work on any previous version of the GlassFish application server.

2.3.2 Deployment of the Online Collection Software application

Once all application prerequisites are in place, including the database preparation, cryptography initialisation and configuration of JEE resources, the OCS application can be deployed on the application server.

The OCS application is bundled as a single Enterprise Application Archive: `oct-ear.ear`.

The application archive must be installed on the application server using one of the facilities provided by the middleware. The most common ways of deployment are through an administration console, by copying the application file to an auto-deploy directory of the server, or by using a command-line tool from the application server distribution.

3 Administration interface

3.1 Access to the interface and choice of the interface language

When connecting to the administration interface of the system you are first presented with the log in screen. The system uses two step authentication, it asks for the username, password and a response to a challenge string of hexadecimal characters (figure 1).

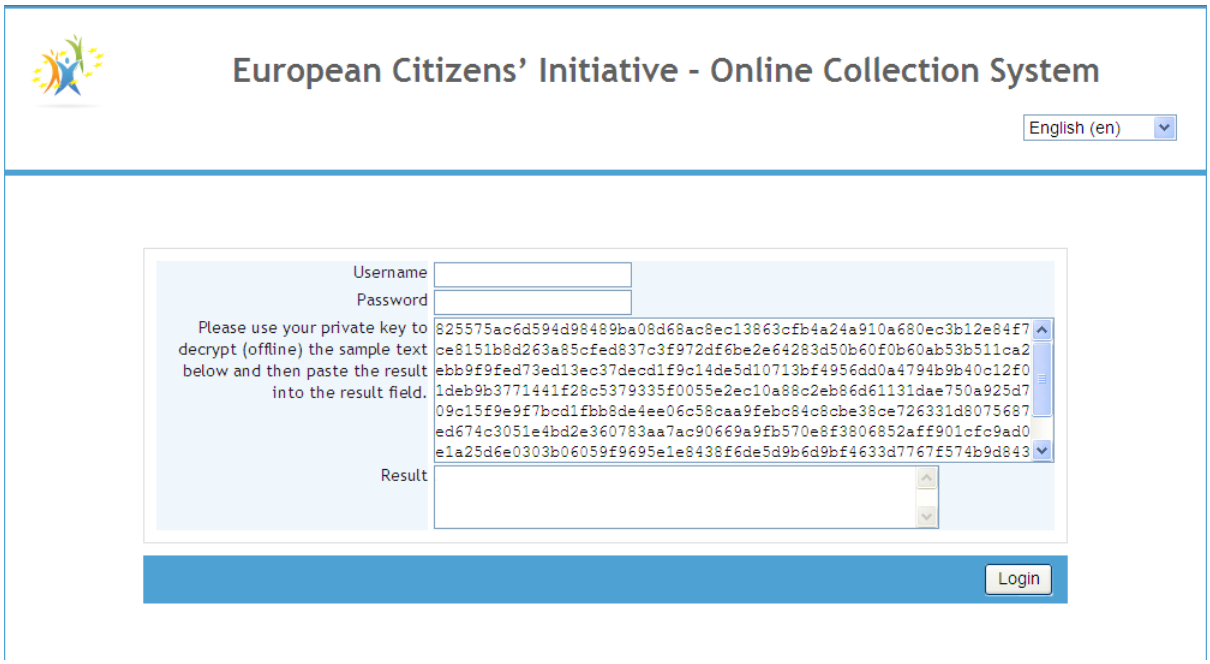


Figure 1: System login screen

To access the system, proceed as follows:

1. Enter your username
2. Enter your password
3. Place the cursor in the text area of the hexadecimal characters then click right and *Select all*, click right again and select *Copy*.
4. Open the cryptography tool and paste, by pressing **ctr^V**, the copied character set for decryption (please refer to section 2.2.2 Cryptography tool installation)
5. Copy the result of the decryption, by pressing **ctr^C,** and go back to the system login page. Place the cursor in the result field, and paste the copied result into the field.
6. Press the button *Login*
7. If the login is successful, the system displays the administration home page (figure 2 below)
8. If the login fails, the system will display the corresponding message. In this case you need to repeat steps 1 to 6 to attempt a new login.

By default, your system is in **offline mode**. In this mode, the public interface of your system is password-protected to prevent public access. This mode therefore allows you to prepare your system in view of its certification prior to starting the collection. Once your system has been configured and certified, you may officially start collecting statements of support via the public interface. For that, you will need to go into online mode via the *System Status* entry in the menu. For more details please refer to section 3.3.1.
In addition, by default, the statement of support form in the public interface is disabled ("Collection OFF"). For more information on the activation/de-activation of the form, see section 3.3.2.

A drop-down list on the top right hand corner of the page allows you to change the language of the interface at any time.

Figure 2: System administration homepage

3.2 Configure the software for your proposed citizens' initiative

In order to configure your system for your proposed citizens' initiative, you have to use the *Initiative setup* entry in the menu. This section will allow you to add the information on your proposed citizens' initiative.

3.2.1 If you have not yet registered your proposed initiative with the Commission

If you are preparing your online collection system and intend to get it certified before registering your proposed citizens' initiative on the ECI register, you have to enter the information on your proposed initiative using the *Enter/Edit information manually* button.

You do not have to complete all information straight away. However you will need to indicate the exact title of your initiative prior to requesting certification of your system by the relevant national authority. This title should be exactly the same as what you intend to register in the European Commission's website ("ECI register"). Please also indicate the language in which you will be registering the initiative.

Note: the possibility to enter data manually only exists in offline mode.

3.2.2 If you have already registered your proposed initiative with the Commission

In this case, you can upload the XML file containing the information on your proposed initiative, which will be available in your organiser account in the ECI register as soon as the registration of your proposed initiative has been confirmed by the European Commission. See the following section for instructions on how to upload the file.
Please note that you will only be able to put the system in online mode after having uploaded the XML file: this will ensure that the data used in your online collection system corresponds exactly to the information registered in the ECI register.

3.2.3 *Upload the file downloaded from the ECI register*

In order to do so, you have to:
1. Go to your organiser account in the ECI register.
2. Download the file available in the *Manage your initiative* menu (*Set up your online collection system* entry) and save it on your local drive.
3. Access the OCS *Initiative setup* page of the administration interface, click on the *Upload file* button (you need to be logged in first)
4. Click on the *Browse* button to locate the file on your computer and click on the *Open* button 5. Click on the *Upload* button.

Please note that once you go into online mode, the data on your proposed initiative cannot be altered anymore. You will then only be able to add new language versions of your proposed initiative uploading the above XML file (see next section).

3.2.4 Add the language versions published in the ECI register for your proposed initiative

To add the language versions you have provided and that have been published on the ECI register, you have to make a new download in your organiser account of the file containing the information on your proposed citizens' initiative and upload this new file in the software, as described above. The file contains all language versions published for your proposed initiative at the time of its download, including the registration language.
You can therefore repeat the operation each time new language version(s) are added in the ECI register.
Please note that you do not need to stop the collection in the public interface to upload a new file for your proposed initiative.

In brief:

- In offline mode (you are testing the system), you can either enter data manually or upload the file you will find in your organiser account if you have already registered your proposed initiative with the Commission.

- To go into online mode and once you are in online mode (the collection of statements of support is ongoing), you can only upload the file available in your organiser account.

- You will have to download this file from your account and upload it in your system each time the a new language version for your initiative is published on the ECI register so that this language version is added to your system.

3.3 Manage your system (System status options)

The section refers to the *System status* entry in the menu.

3.3.1 Transition to the online mode (irreversible)

Once your system is ready and has been certified by the competent national authority and once the registration of your proposed citizens' initiative has been confirmed by the Commission, you can go into online mode in order to start collecting statements of support from signatories.
In order to do so, you first have to:
- finalise the initiative setup of the system by uploading the file you will have previously downloaded in your organiser account in the ECI register (you cannot go into online mode if you have entered data manually) and
- upload, in the *System status* entry in the menu, the certificate of conformity of your system you will have received from the competent authority.

Then, in *System status*, you can tick the box *Go into online mode* and click on *Continue*.

Be aware that going into online mode is IRREVERSIBLE and it implies that:
- the information on your initiative including the different language versions is considered as final and you will not be able to modify it anymore. However you will be able to update your initiative setup with any new language versions you add to the ECI register.
- all test signature data you may have used in offline mode are erased.

In addition, by default, the system will automatically enable the statement of support form on the public interface (if the collection is at that time OFF, it will automatically be turned ON). See the section below for more information.

3.3.2 Collection mode: ON/OFF

In both offline and online modes, you can choose to activate or de-activate the statement of support form in the public interface. This enables you to allow or prevent the submission of statements of support via the public interface.

When the collection is OFF, the public interface homepage is still accessible but not the form itself (the *Support* button giving access to the form is not available).
When the system is offline, the general public does not have access to the system, but you may want to activate the statement of support form in order to test the collection.
You can activate or de-activate the form at any time. It does not have any impact on the statements of support already collected.

In order to change the collection mode, select ON or OFF by ticking the corresponding box in the *System status* page and click on *OK*.
Please note that by default, the collection is OFF in offline mode and ON in online mode.

3.4 Monitor and export statements of support collected

This section allows you to monitor the collection of statements of support submitted through the public interface of the system and to export the corresponding data.
This section is available in both offline and online modes.

The data are encrypted in the system. Once exported, you will need to decrypt them using the offline tool in order to be able to analyse them. Please see section 3.4.4 for more information on how to decrypt the exported data.

3.4.1 Current signature distribution

The first part of the page, named *Current signature distribution*, displays the total distribution of signatures, classified according to the country of signatories.

You can export all statements of support collected at any time through the button *Export all*.

Once the export is completed, the exported file will be made available in the file system you have indicated when you have initialised the system (see 2.2.1 Application file storage). The exported files will be automatically classified by country and, for each country, by language version of the initiative selected by the signatory. The folder names are based on the country codes and language codes you will find in **Annexes II and III** respectively.

At the end of your signature collection and if you have reached the required number of signatories, you will have to send the relevant statements of support exported to each competent authority in the member states for verification.

3.4.2 Report by period and/or by country

The second part of this section allows you to make queries reporting statements of support according to the country and/or the date of submission. You can select a period of time by completing the first two fields and/or you can select a country through the drop-down list. Launch the query clicking on the *Count* button.
You can then export the corresponding statements of support through the *Export* button that appears once that the system has completed the query.

3.4.3 Delete specific statements of support

The third part of the page allows you to select one or more statements of support – using the signature identifier – in order to delete it/them through the *Delete* button. You may indicate the date of signature in addition to the signature identifier but this is not mandatory.
A report will indicate whether or not the deletion was successful for each statement of support.
When a signatory has successfully submitted his/her statement of support via the public interface, he/she is informed of the signature identifier of his/her statement of support.
You can also find, in the XML file, the signature identifier corresponding to each statement of support once exported and decrypted.

3.4.4 *How to decrypt the exported data*

- Start the Cryptography tool using the password entered during the initialisation phase as described in section 2.2.2. Click the *Proceed* button next to the *Decrypt exported data* as shown in the image below.

Figure 3: Offline tool for decryption of data

The following window will open:

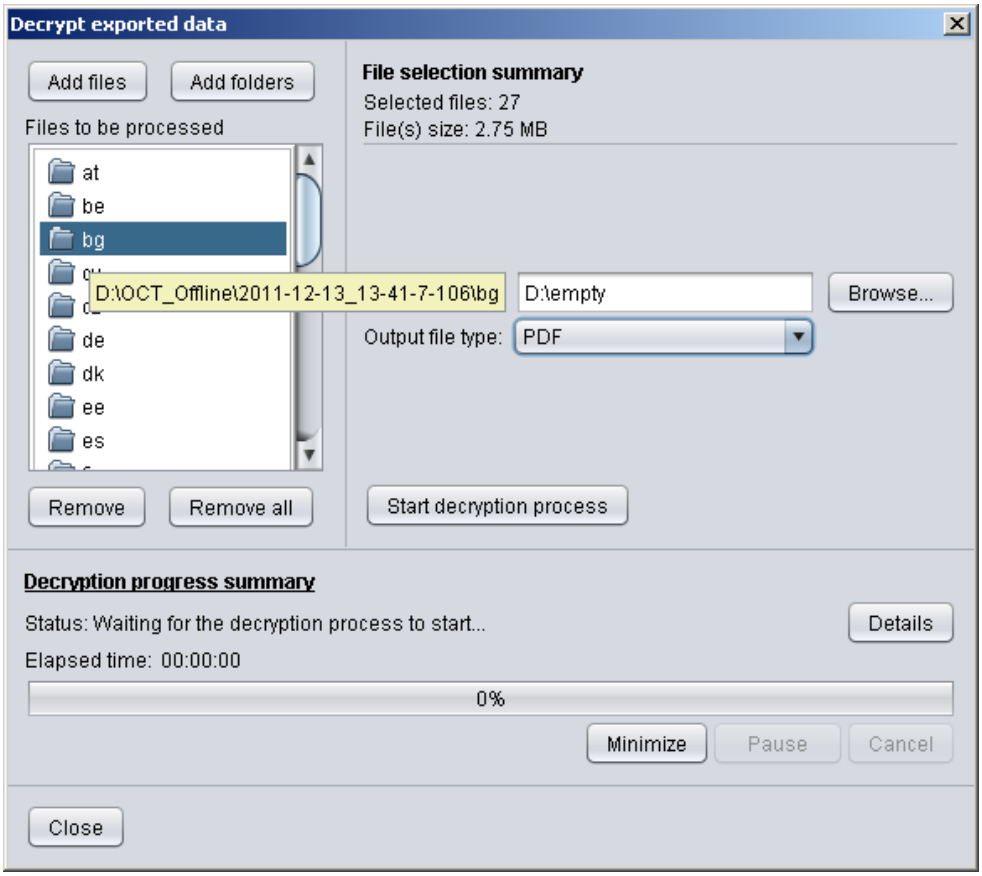


Figure 4: Browsing and selecting folders or files to be decrypted.

- Add the individual files or folders to be decrypted

On the left side-up you can find the buttons for adding new individual files or folders to be processed (*Add files* / *Add folders*).

When adding files, multiple files can be selected with XML file type. When adding folders, only folders can be selected (multiple selection). When going with the mouse over an item from the list of selected files, the full path to the file/folder to that item is displayed.

For removing files/folders there are two possibilities: *Remove all* – which clears the selection of files and folders and *Remove* which removes selected entries individually. For removing multiple files/folders, hold the Control key pressed and click on the files/folders that needs to be removed. Once the selection is made, you can click the *Remove* button or right click the mouse which opens a selection menu from where you can choose *Remove*. Both actions will remove the selected files/folders.

On the right side-up you can find the File selection summary. This part provides you with a summary of all files that will be processed. This is particularly useful when folders are selected. The summary will display the total number of XML files detected on all the folders and sub-folders and files of the selection, together with the total size of those files.

- Choose the output file.

In order to do so, click on the *Browse* button next to the *Output folder* label and select the folder where you would like to have the decrypted files written.

- Choose the output file type from one of the two options: XML or PDF

- Click on *Start decrypt process* in order to proceed with the decryption of the XML files.

After the decryption process has been started, the upper part becomes inaccessible. The *Decryption progress summary* displays the current status of the decrypt process and the elapsed time. Once the decryption process has been started, you can *minimize* the window, *pause* the process, *cancel* the process or see more *details* about it by clicking the appropriate button.
Pause will put the process on a pause state once the file being processed finishes to be processed. That is why, after *Pause* has been pressed, it can take some time until you see that no more progress is done.
On the other side, if you cancel the decryption process, the process gets interrupted immediately and no more files are written to the output.
In order to see the details about a decryption process, press the *Details* button and the below window opens showing in black the total number of files processed, in green the number of files successfully processed and in red the number of files that failed to be processed.

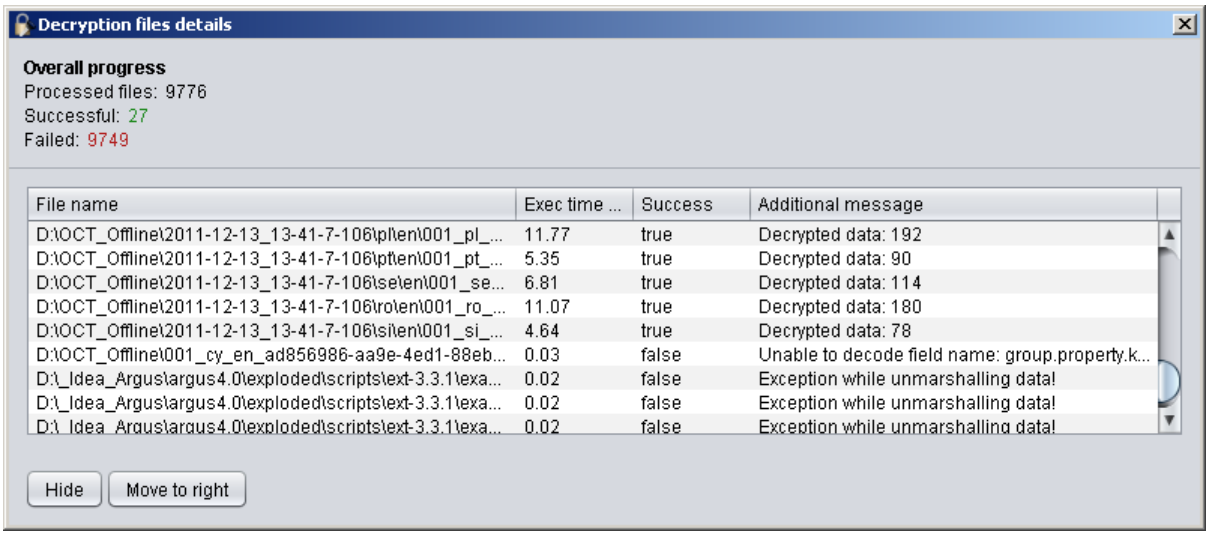


Figure 5: Decryption progress and statistics

For each file processed, a line is added in a table showing the name of the file, the time spent on processing that individual file, the success of the process (true/false) and an additional message as it can be seen on the image above.

4 Public interface

4.1 Access and choice of the interface language

In **offline mode**, the public interface of your system is password-protected to prevent public access. To log in, you have to proceed in the same way as to access the administration part (See section 3.1).

In **online mode**, the interface is publicly accessible and is no longer password-protected. General public will access the homepage of the system through a link on your website.

A drop-down list on the top right of the page allows the public to change the language of the interface at any time.

4.2 Homepage

The homepage is the starting point of the signing-up process. At any moment of the process it is possible to be redirected to it through the *Home* button on the top left of the page.
The homepage provides all the information on your proposed citizens' initiative: it shows the data you provided in the *Initiative setup* in the administration interface, including the different language versions of your proposed initiative.

Figure 6: Homepage of the public interface

The *Support* button on the bottom right of the page allows citizens to start the process of signing-up to your proposed initiative.

4.3 Conformity certificate

From all pages of the public interface, through the relevant button at the top of the page, it is possible for the general public to view the conformity certificate of your online collection system you uploaded via the administration interface (not mandatory in offline mode).

4.4 Privacy statement

From all pages of the public interface, through the relevant button at the top of the page, it is possible for the general public to view the privacy statement concerning signatories' personal data. This privacy statement is part of the official form to support a European citizens' initiative.

4.5 Signing-up

4.5.1 First step: selection of country

Clicking on the *Support* button, signatories access the statement of support form. First of all, they are required to select the member state, which they come from.

The member state selected by signatories may be either their country of residence or their country of nationality. Several links to the ECI website are available where signatories can find more information on the modalities and the requirements for signing-up to a citizens' initiative.

However, once the country is selected, the system informs the signatory that it is possible to sign up only if, depending on the member state:
- they are permanent residents in this country;
or
- they are permanent residents in or citizens of this country;
or
- they are permanent residents in or citizens of this country, included citizens living abroad provided that they have informed the national authorities about their place of residence;
or
- they hold the identification document/number or one of the identification documents/numbers required by this country: in this case additional fields appear to allow signatories to select the relevant document and provide its number.

It is possible to modify the member state chosen using the button *Change* that appears next to the country selected.

In any case, signatories are allowed to sign only once for each proposed citizens' initiative. Note that the system does not allow duplicate statements of support.

4.5.2 Second step: statement of support form

Once the country has been selected, the relevant form to be completed by the signatory appears on the same page. Each form is customised according to the data required by the member state selected.

4.5.3 Third step: finalising and submitting

Once the form has been completed, signatories are required to confirm that the information provided is correct and that they have not already supported your proposed citizens' initiative. They also have to confirm they have read the privacy statement.

To finalise the process, signatories are required to enter the characters they see in the captcha image.

Signatories can then click on the *Submit* button in order to finalise the submission of their statement of support. At any time of the process, signatories are allowed to go back to the previous

page by clicking on the *Back* button, at the end of the page: should they decide to do so, all data already entered will be deleted.

If no error occurs, the system notifies the signatory that the form has been successfully submitted. In addition to this notification, the date and the signature identifier appear on the last page. Finally signatories can return through the relevant link to the organisers' website in the language version selected for the initiative.

Annex I

List of requirements for using the software

- J2EE5 compliant application server
- Relational database, SQL 99 compliant
- File system
- Java 1.5 JDK to run the OCS Crypto Tool

Annex II

Country codes

Short name, source language(s) (geographical name)	Short name in English (geographical name)	Country code
Belgique/België	Belgium	BE
България	Bulgaria	BG
Česká republika	Czech Republic	CZ
Danmark	Denmark	DK
Deutschland	Germany	DE
Eesti	Estonia	EE
Éire/Ireland	Ireland	IE
Ελλάδα (*)	Greece	EL
España	Spain	ES
France	France	FR
Italia	Italy	IT
Κύπρος (*)	Cyprus	CY
Latvija	Latvia	LV
Lietuva	Lithuania	LT
Luxembourg	Luxembourg	LU
Magyarország	Hungary	HU
Malta	Malta	MT
Nederland	Netherlands	NL
Österreich	Austria	AT
Polska	Poland	PL
Portugal	Portugal	PT
România	Romania	RO
Slovenija	Slovenia	SI
Slovensko	Slovakia	SK
Suomi/Finland	Finland	FI

Sverige	Sweden	SE
United Kingdom	United Kingdom	UK

Annex III

Language codes

Source language title	English title	ISO code
български	Bulgarian	bg
español	Spanish	es
čeština	Czech	cs
dansk	Danish	da
Deutsch	German	de
eesti keel	Estonian	et
ελληνικά	Greek	el
English	English	en
français	French	fr
Gaeilge	Irish (4)	ga
italiano	Italian	it
latviešu valoda	Latvian	lv
lietuvių kalba	Lithuanian	lt
magyar	Hungarian	hu
Malti	Maltese	mt
Nederlands	Dutch	nl
polski	Polish	pl
português	Portuguese	pt
română	Romanian	ro
slovenčina (slovenský jazyk)	Slovak	sk
slovenščina (slovenski jezik)	Slovenian	sl
suomi	Finnish	fi
svenska	Swedish	sv