CRYPTOGRAPHIC TOOL

Cryptographic tool User Manual

Date:	04/12/2023
Doc. Version:	1.5.0

Commission européenne, B-1049 Bruxelles / Europese Commissie, B-1049 Brussel – Belgium.

Commission européenne, L-2920 Luxembourg.

Document Control Information

Document Control Information

Settings	Value
Document Title:	User Manual for Cryptographic tool version 1.5.0
Project Title:	European Parliament and European Citizens' Initiative Crypto tool
Document Author:	Jérôme Stefanini. DIGIT.
Doc. Version:	1.5.0
Sensitivity:	Document publicly available on internet on the Joinup platform
Date:	04/12/2023

Document history:

The Document Author is authorized to make the following types of changes to the document without requiring that the document be re-approved:

- Editorial, formatting, and spelling
- Clarification

To request a change to this document, contact the Document Author or Owner.

Changes to this document are summarized in the following table in reverse chronological order (latest version first).

Revision	Date	Created by	Short Description of Changes
1.00	30/09/2020	DIGIT-ECI[at]ec[dot]europa[dot]eu	Redesign of the document. Adding more information about how to upgrade the tool to a new version.
1.01	16/12/2020	DIGIT-ECI[at]ec[dot]europa[dot]eu	§2.8. Precision on decrypting the .zip file and not the .enc file inside the zip file
1.3.0	18/03/2023	DIGIT-ECI[at]ec[dot]europa[dot]eu	Adding documentation for EP election. (Merging the EP election and ECI into one user manual) Removal of usage of jdk17
1.3.1	10/05/2023	DIGIT-ECI[at]ec[dot]europa[dot]eu	Adding chapter §3.2 on how to validate file received from other Member States in the context of the EP elections
1.5.0	04/12/2023	DIGIT-ECI[at]ec[dot]europa[dot]eu	Adding chapter § 2.2.3 Validation of the integrity of the downloaded bundle on how to ensure the integrity of the downloaded software by checking the checksum of the software.

TABLE OF CONTENTS

1 INTRODUCTION 4

1.1 Intended Audience 4

1.2 Differences compared to the previous version of the tool. 4

1.3 Context in which the Crypto tool is used for the European Parliament Elections 4

1.4 Context in which the Crypto tool is used for the European Citizens' Initiative. 5

2 INSTALLATION OR UPGRADE OF THE TOOL 5

2.1 Introduction 5

2.2 Installing the tool 5

2.2.1 Hardware requirements 5

2.2.2 Installation procedure 5

2.2.3 Validation of the integrity of the downloaded bundle 6

2.3 Launching the application 6

2.3.1 Using the scripts bundled with the package 6

2.3.2 Alternative options to launch the application 7

2.3.3 Successful launching of the crypto module 7

2.4 Functionalities used 8

2.5 Initialising the crypto module 9

2.5.1 Initialisation 9

2.5.2 Exporting your credentials 10

2.5.3 Importing credentials from other Member States (European Parliament elections only) 11

2.6 Migrating your credentials - Upgrading your application to a new version - Backing up / restoring your credential folders 12

2.6.1 Introduction 12

2.6.2 Accessing your previous credentials / making a backup of your credentials 12

2.7 Restoring your credentials / Copying your previous credentials to the new instances of the tool 12

2.7.1 Procedure to restore the credentials 12

2.7.2 Validating the restore/migration was successful 12

2.8 File decryption 14

3 FILE VALIDATION (ONLY IN THE CONTEXT OF EP ELECTIONS, NOT FOR ECI) 16

3.1 Introduction 16

3.2 How to validate an xml file (mobile or candidate) – Successful validation scenario 16

3.3 Example of an unsuccessful validation – type of log files available 17

3.3.1 EPCryptoToolRequiredDataDetails.log 19

3.3.2 EPCryptoToolRequiredDataStatistics.log 21

3.3.3 EPCryptoToolApplication.log 21

4 ERROR LOG 21

5 APPENDIX A: CRYPTOGRAPHY & BEST PRACTICES 22

6 APPENDIX B: BEST PRACTICES FOR HANDLING THE KEYS 24

1 INTRODUCTION

This user manual describes:

- How to install the tool
- How to upgrade the tool
- How to backup and restore the tool

This version 1.5.0 is compatible with versions 1.30.0, 1.2.3 and 1.2.4. Files encrypted with any of those versions can by decrypted by any of the other versions and vice-versa.

The same tool can be used for both the European Parliament project and for the European Citizens' Initiative project. Only one instance could be used as the tool is only used for decrypting files in the context of the European Citizens' Initiative and is used both for encrypting and decrypting in the case of the European Parliament project (the other MS credentials only needs to be imported in the case of the European Parliament elections and the private MS credential can be used in both projects).

In case a Member State is willing to install this new version of the tool, it is recommended that the Member States keeps his current credentials (refer to chapter§2.6 on how to upgrade a tool). However, if the Member State decides to generate new credentials, please immediately communicate them to the Commission (DIGIT-ECI@ec.europa.eu).

It is possible to install several version of the crypto tool; however, all the instances need to share the same credentials and same password to access the credentials. Chapter §2.7 describe how to align all the instances of the tools.

One of the most critical operation for a Member State is to make a backup of the credentials after they have been generated and save the password to access those credentials safely. If not already done, please perform this operation as soon as possible (see chapter §2.6).

1.1 Intended Audience

This document is intended for Member States representatives that needs to use the crypto tool in the context of the European Citizens' Initiative.

1.2 Differences compared to the previous version of the tool.

Compared to the previous version 1.3.0, this version 1.5.0. brings following main differences:

- The validation checks against the updated requirements that Member States have provided following the 2023 test campaign for the EP elections of 2024
- Labelling and few small fixes discussed in the context of the Member States working groups.
- OpenJDK version of the jdk 8 is used.

1.3 Context in which the Crypto tool is used for the European Parliament Elections

In the context of EP elections, the Member States will use the crypto tool to encrypt/decrypt the files for/from the Member States before uploading/downloading the files to/from the File Exchange Service.

Three different type of files could be encrypted by the Member States for the other Member States:

1. Mobile candidates
2. Mobile voters
3. Any other type of files

The Member States will need to upload/download the encrypted files to/from the S-CircaBC platform and must then use the crypto tool to decrypt/encrypt the files.

Needless to say: in order that the Member State is able to decrypt the file, the sending Member State should have encrypted the file with the public key that corresponds to the Member States Credential. This is the reason why that any changes of the Member States credentials should immediately be communicated to the Commission.

1.4 Context in which the Crypto tool is used for the European Citizens' Initiative.

In the context of ECI, the Commission or the Organisers will use the crypto tool to encrypt the files for the Member States before uploading the files to the File Exchange Service.

Three different type of files could be encrypted by the European Commission or the Organisers:

4. The electronic statements of support including the data of the online form.
5. The electronic statements of support including the eIDAS data (for Member States who have an eID activated compliant with eIDAS).
6. The scanned paper forms.

The Member States will need to download the encrypted files from the S-CircaBC platform and must then use the crypto tool to decrypt the files.

Needless to say: in order that the Member State is able to decrypt the file, the organiser or the Commission should have encrypted the file with the public key that corresponds to the Member States Credential. This is the reason why that any changes of the Member States credentials should immediately be communicated to the Commission.

Contrary to the process of the European Parliament, in the ECI, the Member States do not need to encrypt files. The Annex VI of the ECI regulation that Member States should upload to the file exchange service is a public file and therefore does not need to be encrypted.

2 INSTALLATION OR UPGRADE OF THE TOOL

2.1 Introduction

Installing or upgrading the tool follows the same process: the first step is to install a new version of the tool. In case of an upgrade, the new package must be installed in a different folder from the previous instance of the tool.

It is important not to delete or to overwrite the previous installation for the reason that the previous installation contains the credentials in use and that those credentials should be either copied to the new instance or kept for a period of two years in case organisers or Commission will use the previous version of the credentials.

2.2 Installing the tool

2.2.1 Hardware requirements

- You should have a 64-bit CPU
- Windows 7 or higher
- Minimum recommended RAM is 8 GB

2.2.2 Installation procedure

- Download the latest release of the zip file containing the EP crypto tool from joinup.eu: https://joinup.ec.europa.eu/collection/eparticipation-and-evoting/solution/european-parliament-crypto-tool-software/release/130

- Unzip the file (epcrypto-x.x.zip) containing the EP crypto tool in a folder (in case a previous version of the tool was already installed, choose a different folder).
- Delete the epcrypto-x.x.zip file.

The EP crypto tool is installed.

Remark: To unzip the epcrypto-x.x.zip file, you should install third party software like 7zip (www.7-zip.org/).

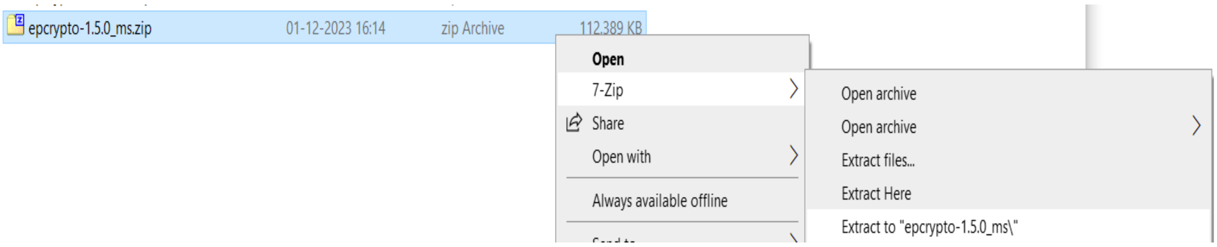
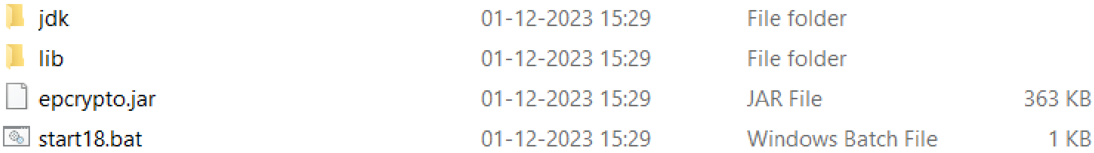


Figure 1 Unzip the file



jdk	01-12-2023 15:29	File folder	
lib	01-12-2023 15:29	File folder	
epcrypto.jar	01-12-2023 15:29	JAR File	363 KB
start18.bat	01-12-2023 15:29	Windows Batch File	1 KB

Figure 2 epcypto.zip file unzipped

2.2.3 Validation of the integrity of the downloaded bundle

In order to ensure that the downloaded bundle has not been corrupted or maliciously changed, it is advised to perform a checksum. See below how to generate this checksum on Windows (supported platform for the crypto tool):

1) Open a command prompt

2) Navigate to the directory where the file is placed (cd C:\example_path) (Tip you can just type "cd " and drag and drop the folder where the file is placed from Windows Explorer to the command pront to insert the path in the command pront).

3) Type the following command "certUtil -hashfile epcrypto-1.5.0_ms.zip SHA256" (replace the part in bold with the name of the file)

4) An output will be generated (e.g for epcrypto-1.5.0_ms.zip it will be 0ed89fe7a8af762003ee9b60b69d784222a82c52e4779111fca13b1028f41ac0):

5) This checksum will also be communicated to Member States via a S-CircaBC notification. Make sure that you compare your checksum with the one contained in the notification.

2.3 Launching the application

2.3.1 Using the scripts bundled with the package

2.3.1.1 Launching with Java 8

The crypto tool has been prepared to be compatible with Java 8. The crypto tool installation package contains the java 8 version with which the tool has been tested.

Launch the tool using the script start18.bat available in the

2.3.1.2 Access rights

The crypto tool is a java application (jar file). In order to guarantee that the application behaves as expected, a working jdk has been packaged and delivered with the tool (see previous chapter).

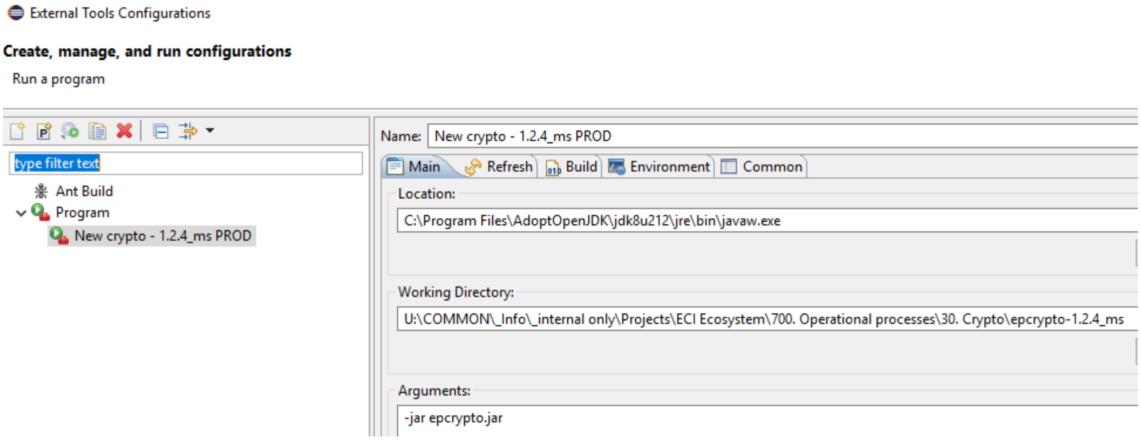
In order to be able to launch the start18.bat, you need to have the permission on your desktop to launch the jdk that has been bundle with the package. In case it does not launch, you should check with your IT support to get the rights to launch the jdk.

2.3.2 Alternative options to launch the application

In some Member States (and at the Commission as well), it could be difficult to get additional permission to launch the application. Alternative options exist however they depend on every Member State IT department.

For example, at the European Commission, there is a way to launch the crypto module without having to request any additional permissions than the default one (which are by default not the one of an administrator): this solution takes advantage that the Eclipse client is available in the Windows 10 EC Store and that this Eclipse client is coming with a jdk that is compatible with the crypto module.

It is then possible to configure the Eclipse client to launch the application. See below the configuration parameters to use the Eclipse client that is used at the European Commission:



External Tools Configurations

Create, manage, and run configurations

Run a program

type filter text

- Ant Build
- Program
  - New crypto - 1.2.4_ms PROD

Name: New crypto - 1.2.4_ms PROD

Main | Refresh | Build | Environment | Common

Location:
C:\Program Files\AdoptOpenJDK\jdk8u212\jre\bin\javaw.exe

Working Directory:
U:\COMMON_Info_internal only\Projects\ECI Ecosystem\700. Operational processes\30. Crypto\epcrypto-1.2.4_ms

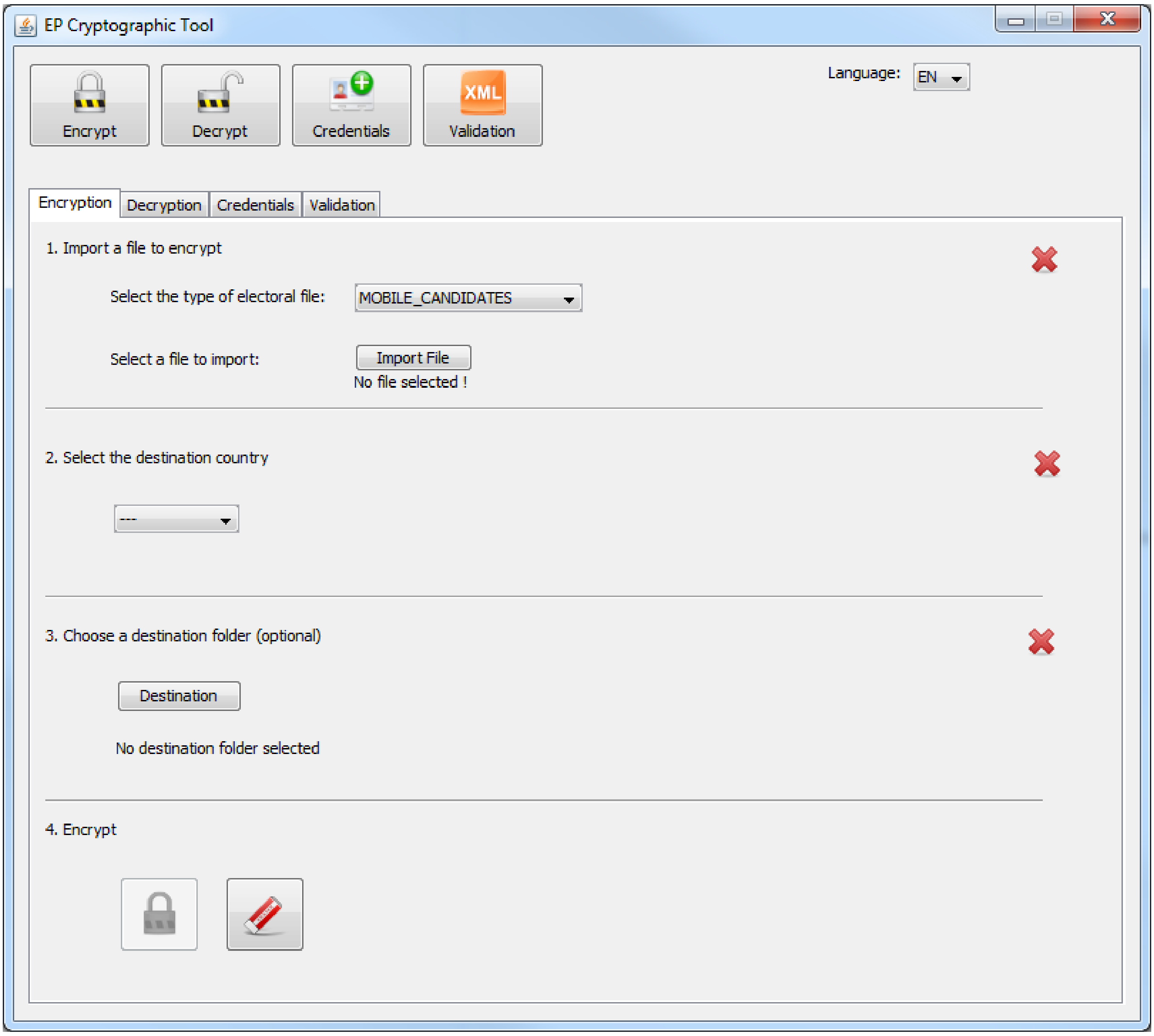
Arguments:
-jar epcrypto.jar

Figure 3 Launching the crypto module with Eclipse at the European Commission

Other alternatives may exist at Member States side (e.g. a jar launcher), please consult your IT support.

2.3.3 Successful launching of the crypto module

See in the below picture what you should see if the application has correctly started.



Language: EN

1. Import a file to encrypt

Select the type of electoral file: MOBILE_CANDIDATES

Select a file to import:

No file selected !

2. Select the destination country

---

3. Choose a destination folder (optional)

No destination folder selected

4. Encrypt

Figure 4 The application has correctly started

2.4 Functionalities used

You can use the navigation bar to navigate inside the application.

There are four navigation buttons. The four of them are used in the context of the European Parliament elections but only two are used by Member States in the context of ECI:

- Encrypt: display the encryption screen (Not needed in the context of ECI)
- Decrypt: display the decryption screen
- Credentials: display the credentials screen
- Validation: (Not needed in the context of ECI)

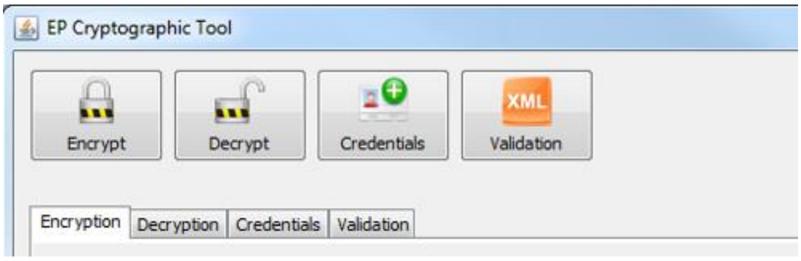


Figure 5 Navigation bar

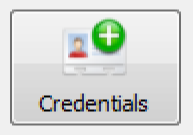
The only current available languages are English [EN] and French [FR].

2.5 Initialising the crypto module

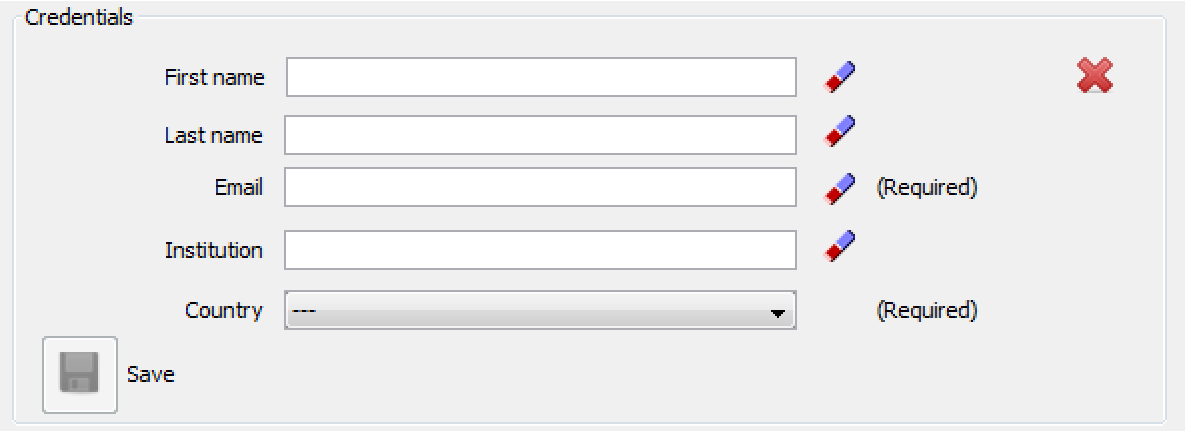
2.5.1 Initialisation

Initialising the crypto module is mandatory whether this is the first ever installation of the crypto module or in the case you are upgrading to a new version.

It is when you initialise that the folder of the Member State is created.

In the navigation bar, select the credentials.  button.

In the credentials section, fill all the fields and save your modifications. (**Make sure you select your country code).**



Credentials

First name		
Last name		
Email		(Required)
Institution		
Country	---	(Required)

Figure 6 Credentials section

In the credentials protection section, define a password and protect your credentials.

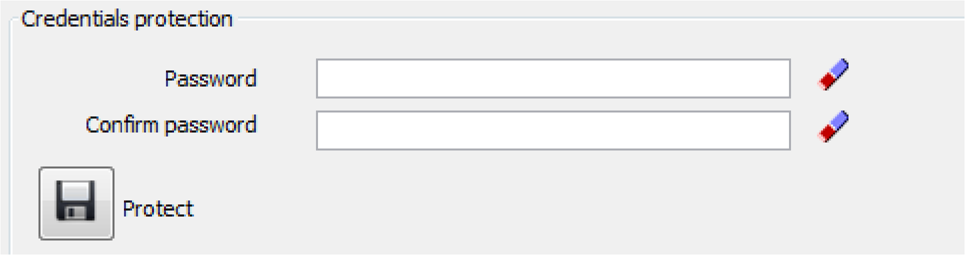


Figure 7 Protect section

Depending on the specifications of your system, this operation can take several minutes. You will see a progress bar indicating that the application is generating the security keys.

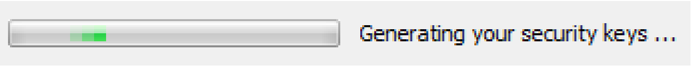


Figure 8 Protection in progress

You will be informed when your credentials are protected.

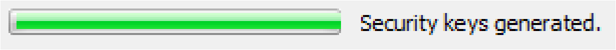


Figure 9 Protection done

Each time you change your password and protect your credentials, this is generating a new set of credentials. So BE EXTREMELY CAUTIOUS and aware of your action and consequences before changing your password.

In the case this is the first installation of the crypto module or you do not plan to restore your previous credentials (see next chapter) you must then export your credentials and send them again to the European Commission DIGIT-ECI@ec.europa.eu

2.5.2 Exporting your credentials

Note: In the case you plan to restore your previous credentials, you do not need to perform again this action. You need to perform this action only if you have changed your credentials and plan to use them.

- Go to the credentials screen (use the navigation screen) and click on 'export credentials' button.

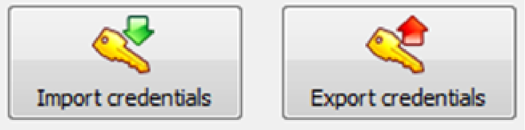
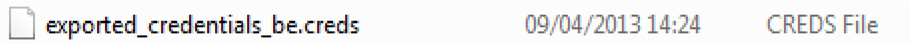


Figure 10 export actions

- You must select a destination folder.

If the application asks you to introduce a password, you must use the one you have defined during the credentials protection.

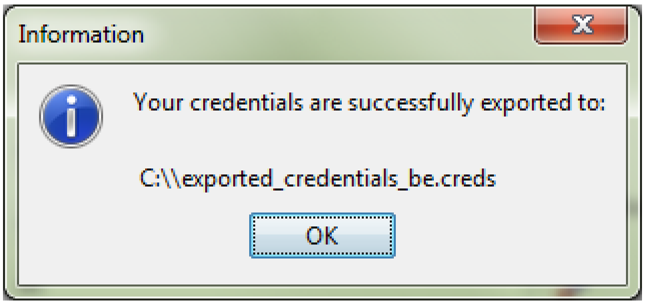
The name of the credentials file has the following format: exported_credentials_(countrycode).creds



exported_credentials_be.creds 09/04/2013 14:24 CREDS File

Figure 11 Exported credentials file

The application will inform you about the status of those two actions:



Your credentials are successfully exported to:

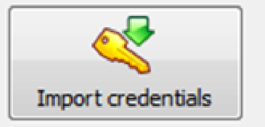
C:\\exported_credentials_be.creds

Figure 12 Credentials export

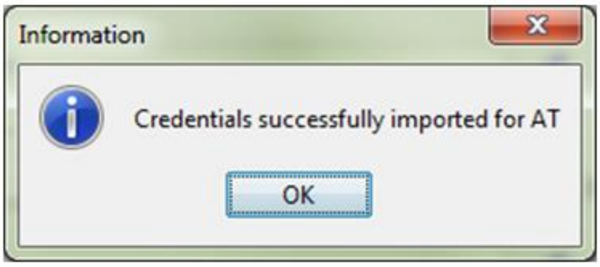
Export restriction: you cannot export your credentials if they are not protected)

2.5.3 Importing credentials from other Member States (European Parliament elections only)

- Go to the credentials screen (use the navigation screen)
- and click on Import credentials



- Select the credentials to import
- You should receive a notification that the credentials has been successfully imported (see below example after importing the Austrian credentials)



Credentials successfully imported for AT

Figure 12 Credentials import

2.6 Migrating your credentials - Upgrading your application to a new version - Backing up / restoring your credential folders

2.6.1 Introduction

This chapter deals about:

- Migrating your credentials to another instance of the tool (whether you decided to install the tool on another desktop or on a different location (shared drive, personal drive)
- Upgrading your application to a new version of the crypto tool
- Backing up / restoring your credentials in case you realise that you cannot access your credentials anymore or that your password is incorrect.

2.6.2 Accessing your previous credentials / making a backup of your credentials

The Member States should have backed up the following files after they have installed and configured the first version of the tool.

The backup of the credentials is performed by saving the following directory

- **[rootfolderofMS]\data**

2.7 Restoring your credentials / Copying your previous credentials to the new instances of the tool

2.7.1 Procedure to restore the credentials

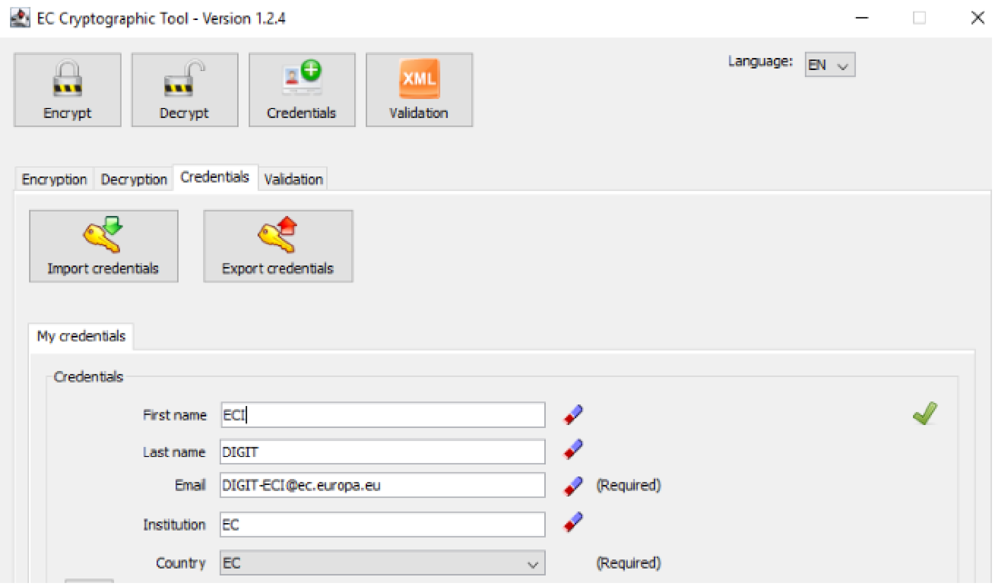
The credentials are then restored by overwriting in the new instance of the crypto tool the folder [rootfolderofMS]\data with the backed up folder [rootfolderofMS]\data

Note: in order that the instance of the crypto tool contains a subfolder data, you need to complete the set-up of the new instance by creating temporary credentials and saving the password as described in §2.5.1. Those credentials and password will be replaced by the old credentials and password after the restore has been completed.

2.7.2 Validating the restore/migration was successful

Launch the new instance of the Crypto tool.

The first indication that the restore was successful is that you should see your previous credentials displayed again (see figure below in the case of the European Commission instance):



First name: ECI

Last name: DIGIT

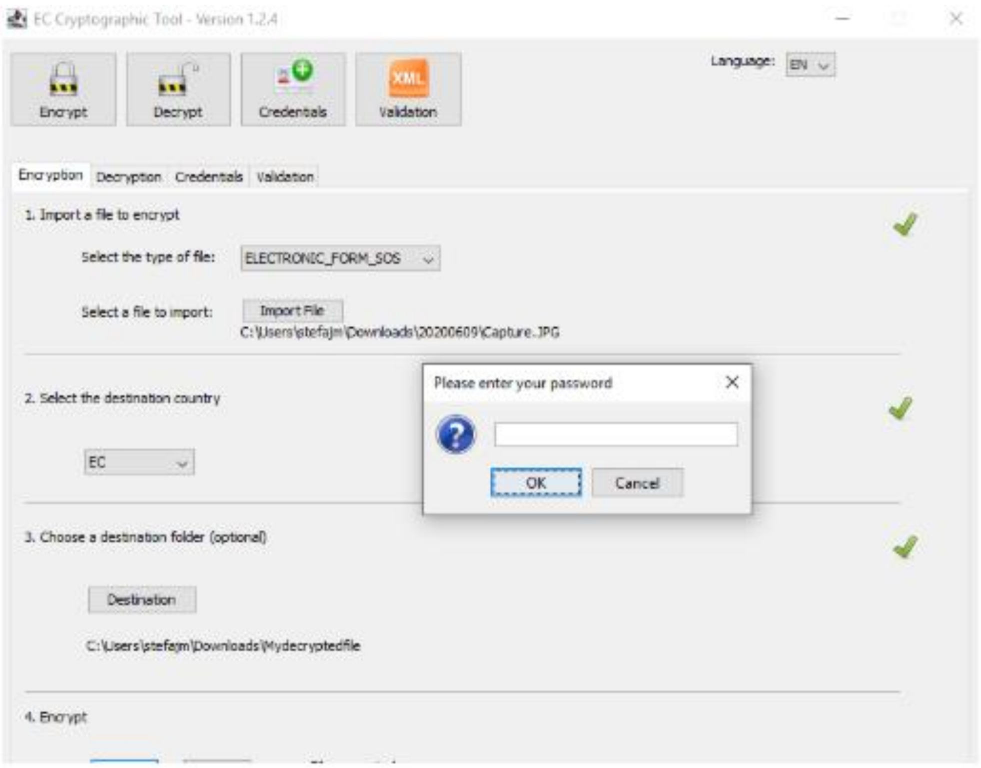
Email: DIGIT-ECI@ec.europa.eu (Required)

Institution: EC

Country: EC (Required)

Figure 13 Example of restored credentials in case of the European Commission instance of the tool

The second test that you can perform is to try to encrypt a file for your own MS.



1. Import a file to encrypt

Select the type of file: ELECTRONIC_FORM_SOS

Select a file to import: C:\Users\stefajm\Downloads\20200609\Capture.JPG

2. Select the destination country

EC

3. Choose a destination folder (optional)

C:\Users\stefajm\Downloads\Mydecryptedfile

4. Encrypt

Figure 14 trying to decrypt a file by providing the previous password

You are requested to provide a password to perform the decryption. The password of your previous credentials should now be active on this new instance and the encryption should be successful.

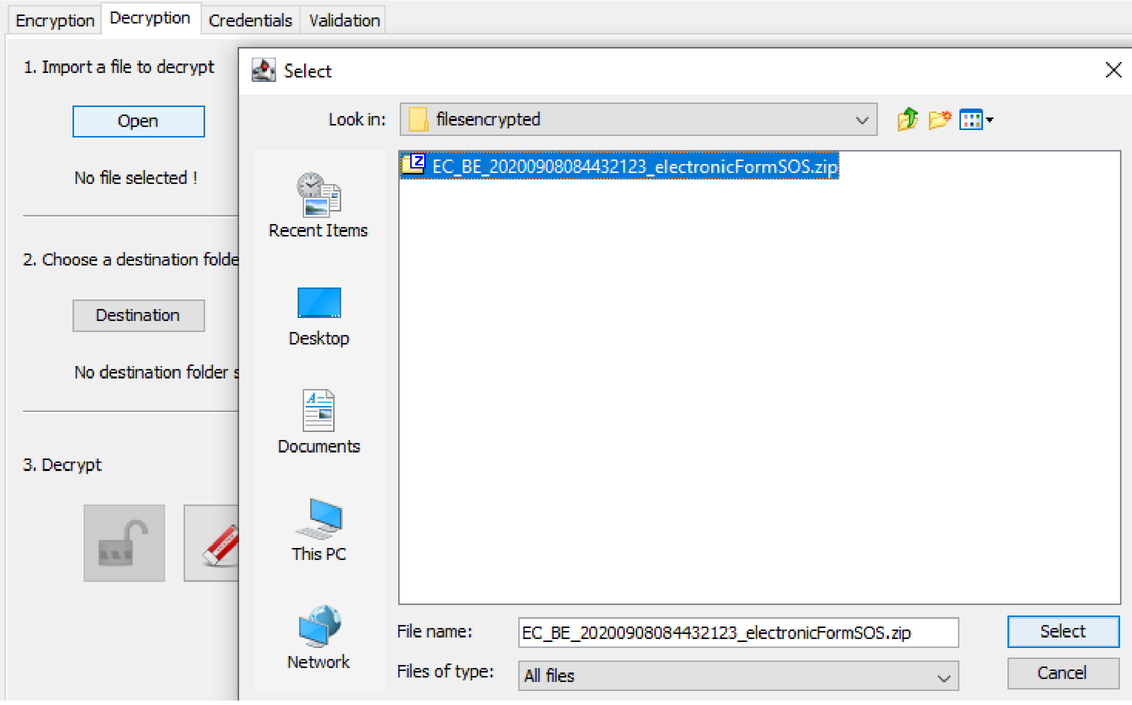
This should prove that the new installation uses now the same credentials that you managed to restored.

2.8 File decryption

To decrypt a file, follow the following steps:

1. Go to the decryption screen (click on ’decrypt‘ in the navigation bar).
2. Select the file to decrypt

   Note: the file to select and to decrypt is the zip file that you receive (e.g. EC_BE_20200908084432123_electronicFormSOS.zip) in no case you should try to unzip the file and try to decrypt the .enc file inside the .zip, it will not work…



No file selected !

No destination folder s

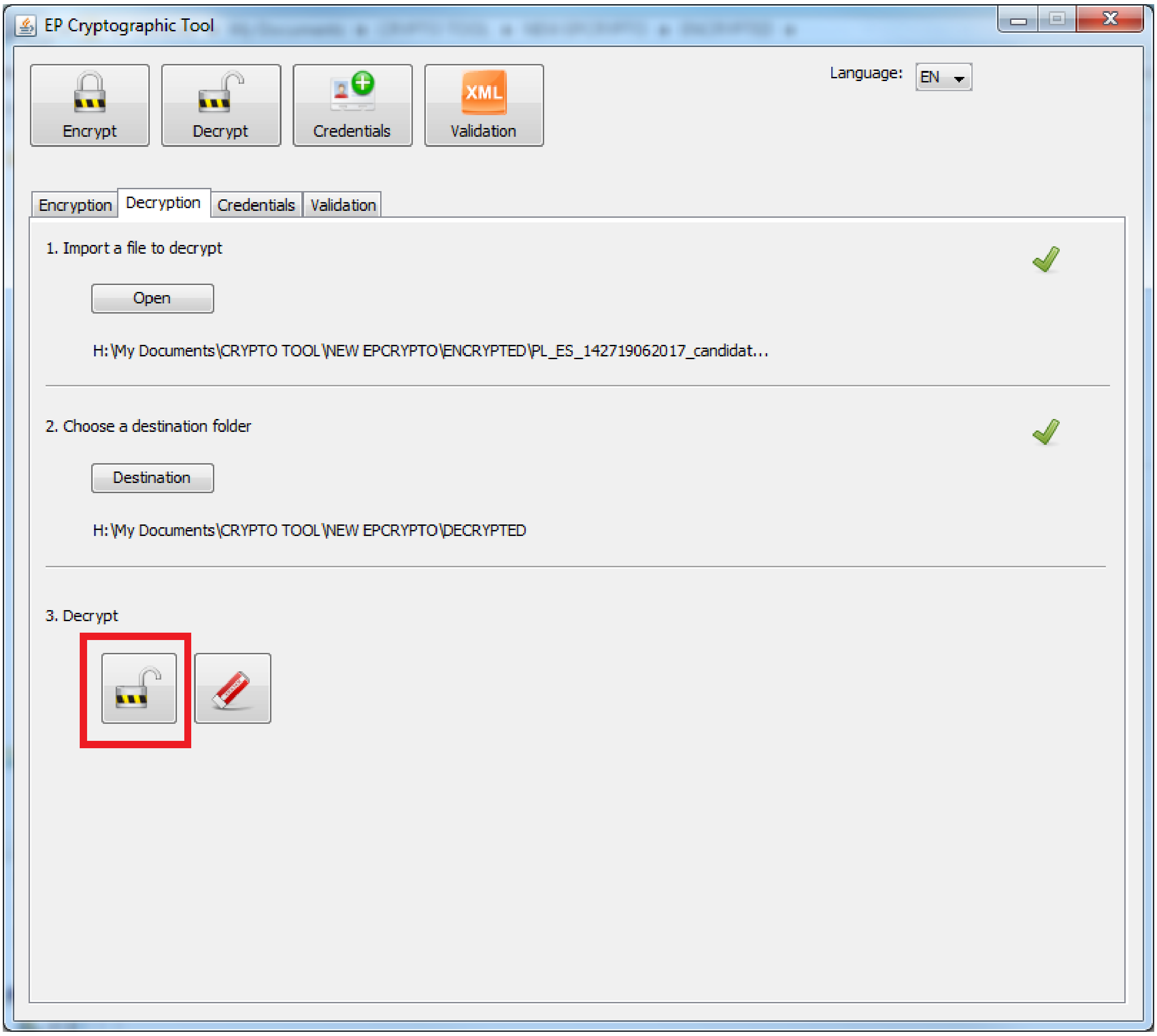
Look in: filesencrypted

EC_BE_20200908084432123_electronicFormSOS.zip

File name: EC_BE_20200908084432123_electronicFormSOS.zip

Files of type: All files

3. Select the destination folder for the decrypted file
4. In the decrypt section, click the ’decrypt‘ button in the left bottom of the screen.
5. Enter your credentials passwords when prompted for it.



1. Import a file to decrypt ✓

H:\My Documents\CRYPTO TOOL\NEW EPCRYPTO\ENCRYPTED\PL_ES_142719062017_candidat...

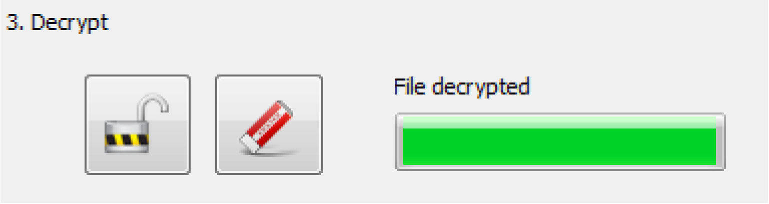
2. Choose a destination folder ✓

H:\My Documents\CRYPTO TOOL\NEW EPCRYPTO\DECRYPTED

3. Decrypt

Figure 15 File decryption

The application displays a message when the decryption process is complete.



3. Decrypt

File decrypted

Figure 16 File decrypted

3 FILE VALIDATION (ONLY IN THE CONTEXT OF EP ELECTIONS, NOT FOR ECI)

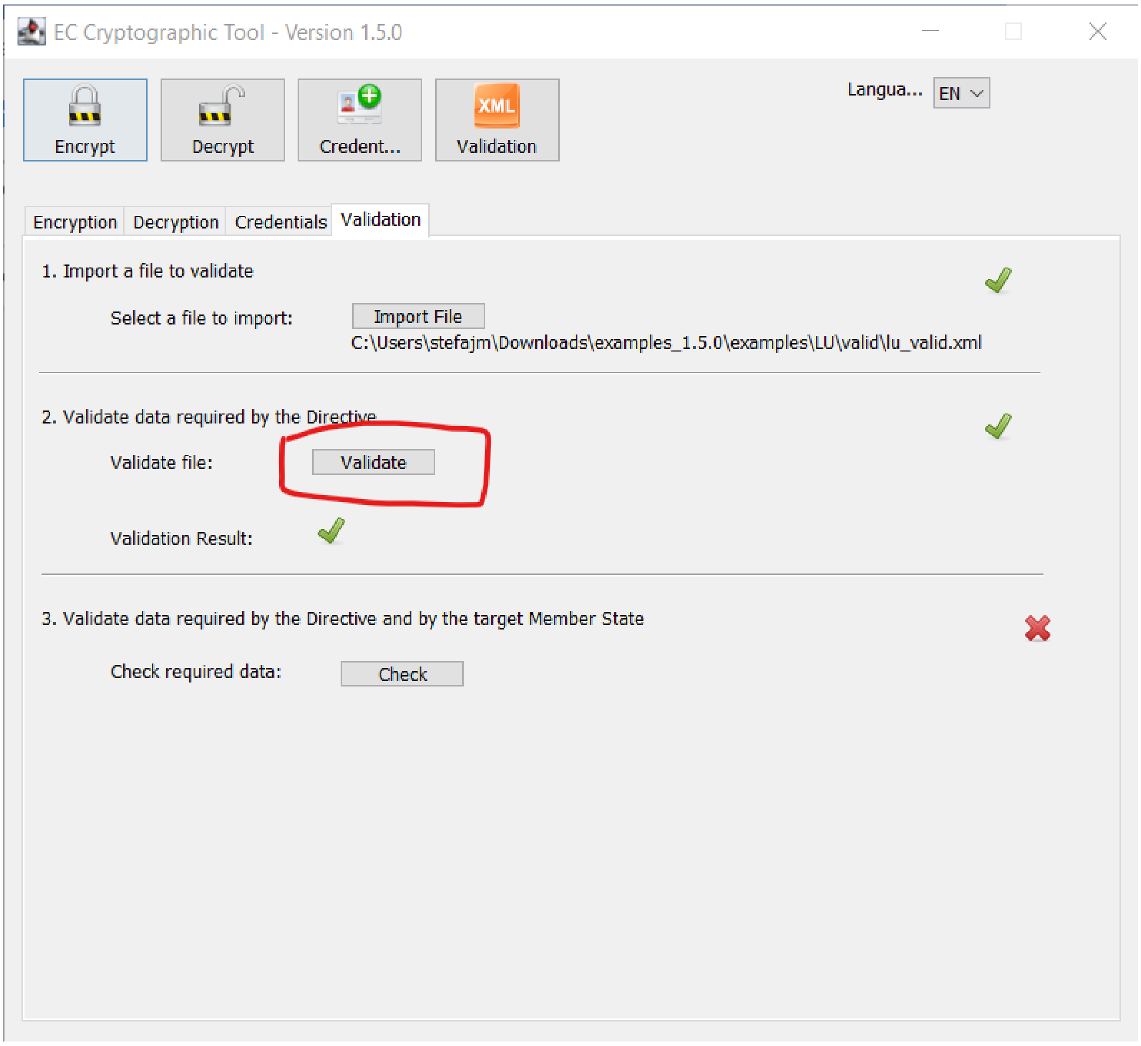
3.1 Introduction

In the context of the EP elections, the crypto tools gives the possibility to validate the xml files that a given MS will send to the other MS or to validate the correctness of the files received from other MSs.

This check is made against the requirements that are laid down in the currents legislative basis (currently Directive 93/109/EC) or that have been provided by Member States (refer to the S-CircaBC platform for the last version of the personal data requirements by Member States)

3.2 How to validate an xml file (mobile or candidate) – Successful validation scenario

1. Go to the validation screen (click on Validation in the navigation bar).
2. Import a XML exchange file (usually to be sent to another Member State or a file received from another Member State that has been previously decrypted) to be validated against the requirements of the d Directive 93/109/EC
3. Click on Validate.
4. Tool displays validation result.



1. Import a file to validate ✓

Select a file to import: C:\Users\stefajm\Downloads\examples_1.5.0\examples\LU\valid\lu_valid.xml

2. Validate data required by the Directive ✓

Validate file:

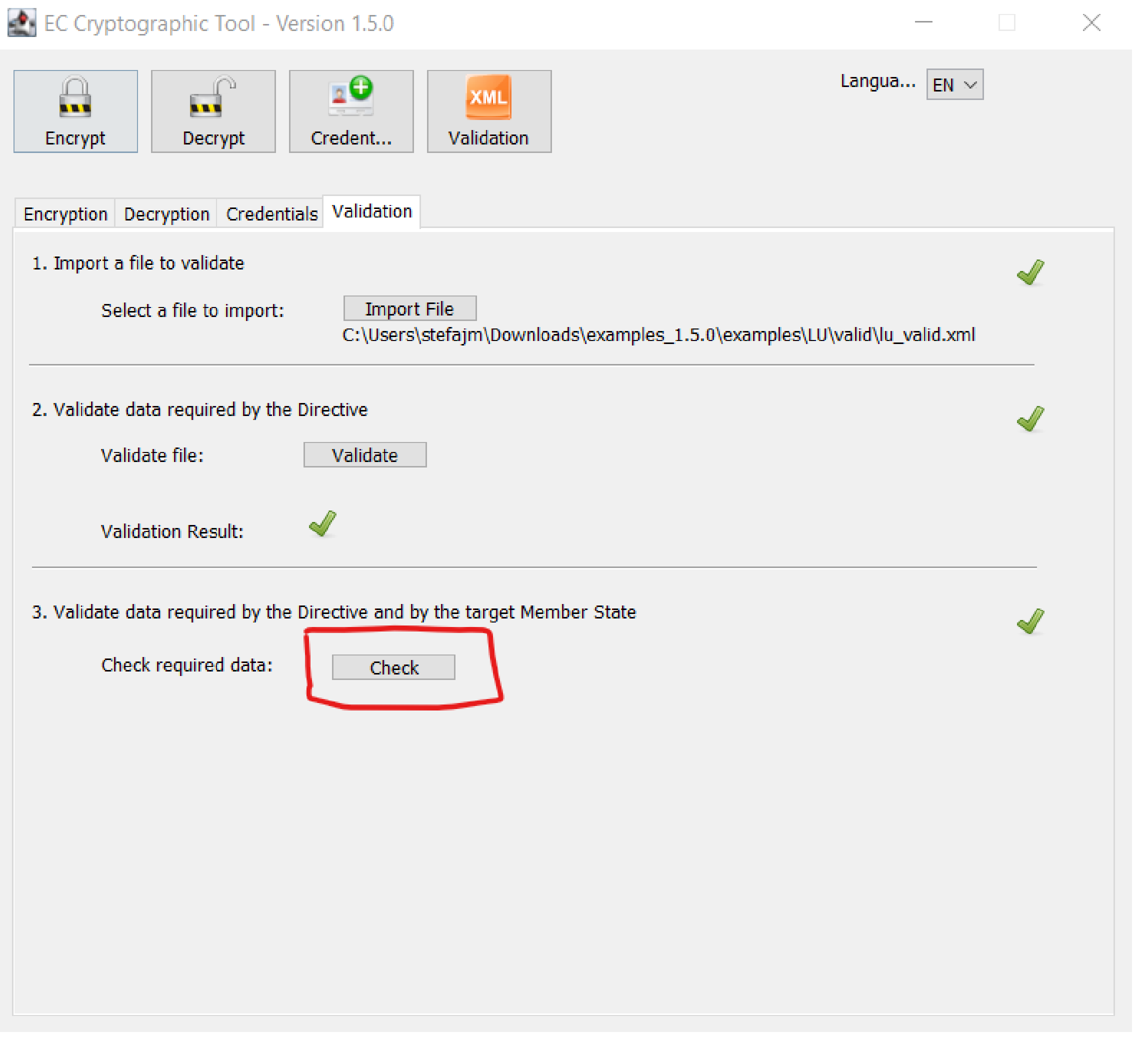
Validation Result: ✓

3. Validate data required by the Directive and by the target Member State ✗

Check required data:

Figure 17 Positive file validation against official exchange schema

5. In case of successful validation select Check button to validate data in the file against the requirements provided by the Member States (currently compiled in table Table-MS_V3-v2.docx)
6. In the below example, the tool display a positive validation result.



EC Cryptographic Tool - Version 1.5.0

1. Import a file to validate ✓

Select a file to import: Import File
C:\Users\stefajm\Downloads\examples_1.5.0\examples\LU\valid\lu_valid.xml

2. Validate data required by the Directive ✓

Validate file: Validate

Validation Result: ✓

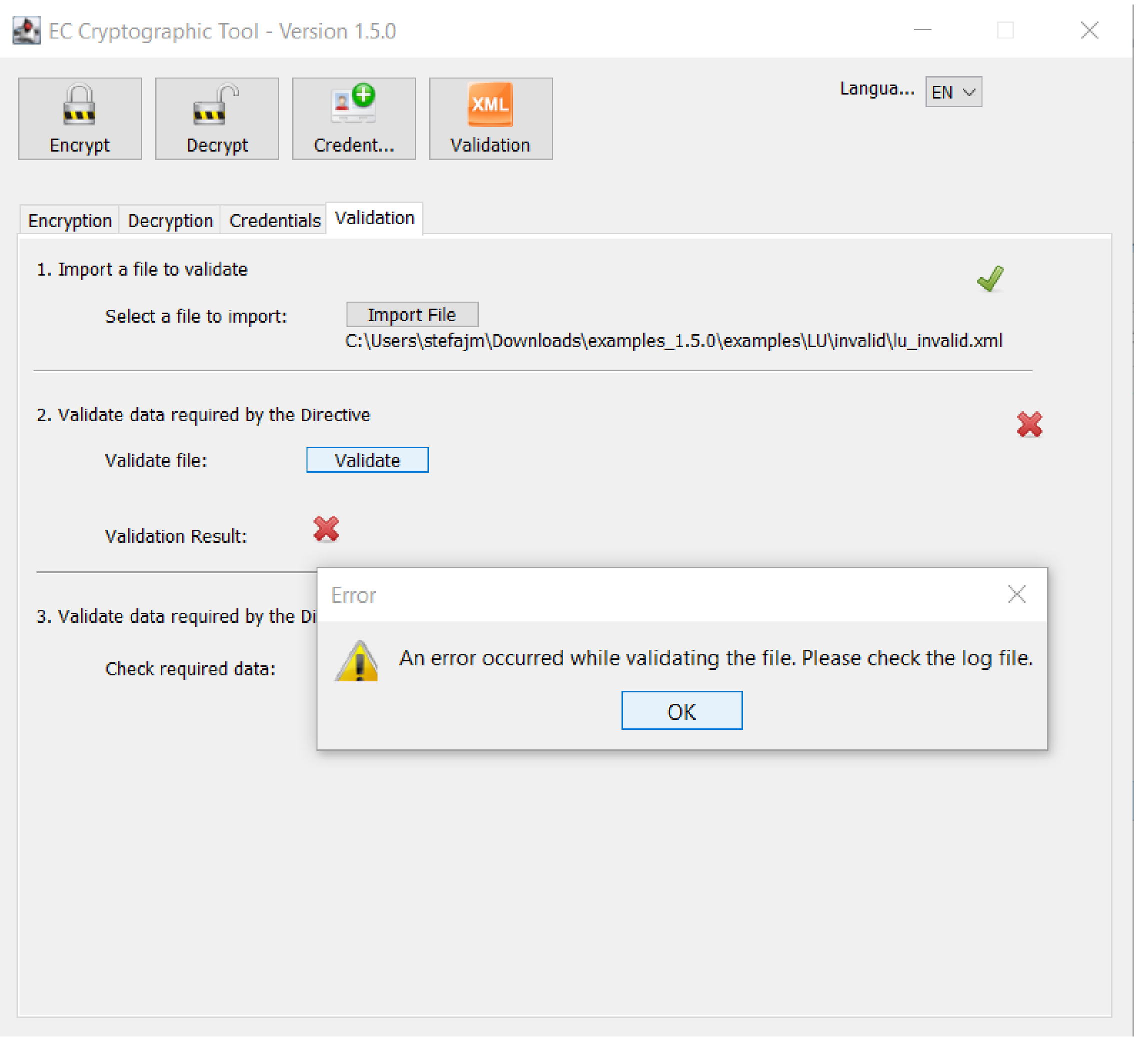
3. Validate data required by the Directive and by the target Member State ✓

Check required data: Check

Figure 18 File validation of data against Annex V

3.3 Example of an unsuccessful validation – type of log files available

In the case the xml would not be valid, below is the error message that you will see in case the unsuccessful validation occurs at the first validation or at the second stage of the validation.



EC Cryptographic Tool - Version 1.5.0

1. Import a file to validate

Select a file to import: C:\Users\stefajm\Downloads\examples_1.5.0\examples\LU\invalid\lu_invalid.xml

2. Validate data required by the Directive

Validate file:

Validation Result: ✗

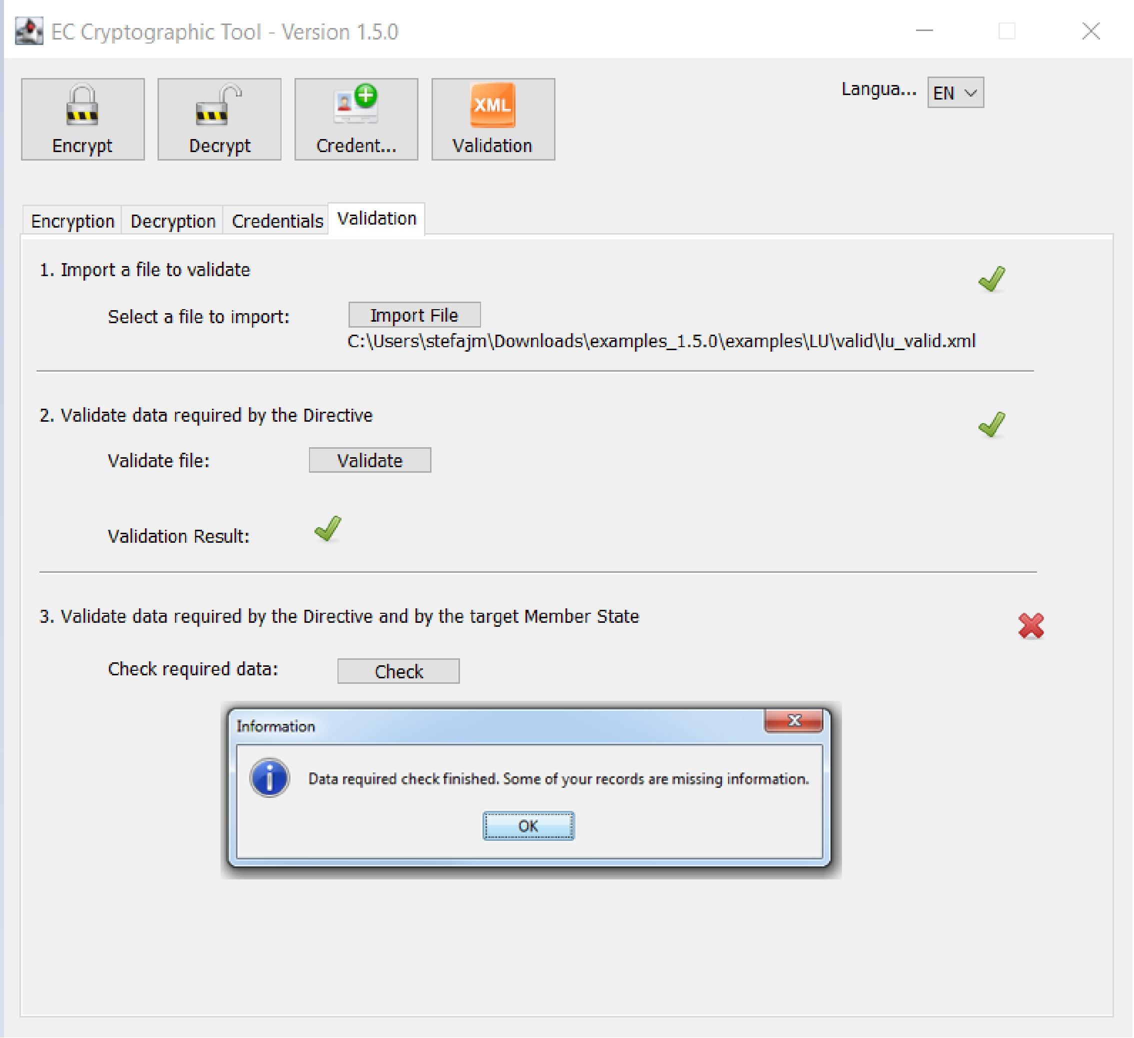
3. Validate data required by the Di

Check required data:

Error

An error occurred while validating the file. Please check the log file.

Figure 19 Schema validation error against directive requirement



1. Import a file to validate

Select a file to import: Import File
C:\Users\stefajm\Downloads\examples_1.5.0\examples\LU\valid\lu_valid.xml

2. Validate data required by the Directive

Validate file: Validate

Validation Result: ✓

3. Validate data required by the Directive and by the target Member State

Check required data: Check

Information

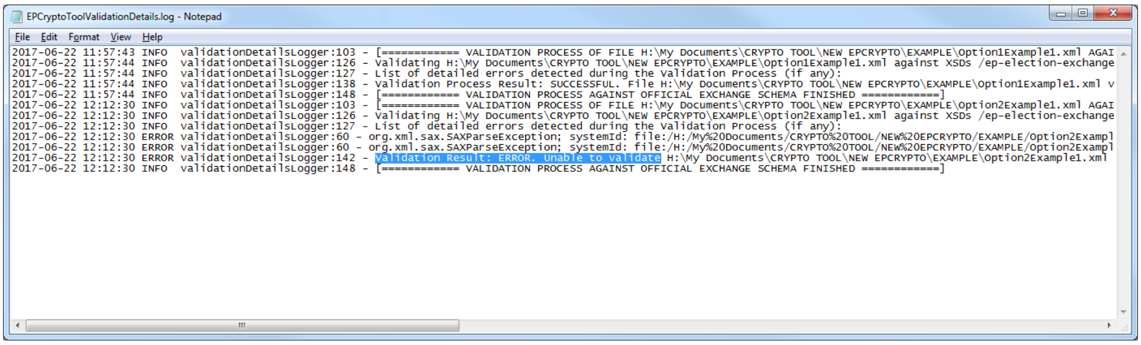
Data required check finished. Some of your records are missing information.

OK

Figure 20 File validation of data against Member States personal data requirements

3.3.1 EPCryptoToolRequiredDataDetails.log

In both cases, it is advised to look in the logs of the application and especially in EPCryptoToolRequiredDataDetails.log (see below screenshot)


EPCryptoToolValidationDetails.log - Notepad
File Edit Format View Help

```
2017-06-22 11:57:43 INFO  validationDetailsLogger:103 - [============ VALIDATION PROCESS OF FILE H:\My Documents\CRYPTO TOOL\NEW EPCRYPTO\EXAMPLE\Option1Example1.xml AGAI
2017-06-22 11:57:44 INFO  validationDetailsLogger:126 - Validating H:\My Documents\CRYPTO TOOL\NEW EPCRYPTO\EXAMPLE\Option1Example1.xml against XSDs /ep-election-exchange
2017-06-22 11:57:44 INFO  validationDetailsLogger:127 - List of detailed errors detected during the Validation Process (if any):
2017-06-22 11:57:44 INFO  validationDetailsLogger:138 - Validation Process Result: SUCCESSFUL. File H:\My Documents\CRYPTO TOOL\NEW EPCRYPTO\EXAMPLE\Option1Example1.xml v
2017-06-22 11:57:44 INFO  validationDetailsLogger:148 - [============ VALIDATION PROCESS AGAINST OFFICIAL EXCHANGE SCHEMA FINISHED ============]
2017-06-22 12:12:30 INFO  validationDetailsLogger:103 - [============ VALIDATION PROCESS OF FILE H:\My Documents\CRYPTO TOOL\NEW EPCRYPTO\EXAMPLE\Option2Example1.xml AGAI
2017-06-22 12:12:30 INFO  validationDetailsLogger:126 - Validating H:\My Documents\CRYPTO TOOL\NEW EPCRYPTO\EXAMPLE\Option2Example1.xml against XSDs /ep-election-exchange
2017-06-22 12:12:30 INFO  validationDetailsLogger:127 - List of detailed errors detected during the Validation Process (if any):
2017-06-22 12:12:30 ERROR validationDetailsLogger:60 - org.xml.sax.SAXParseException; systemId: file:/H:/My%20Documents/CRYPTO%20TOOL/NEW%20EPCRYPTO/EXAMPLE/Option2Exampl
2017-06-22 12:12:30 ERROR validationDetailsLogger:60 - org.xml.sax.SAXParseException; systemId: file:/H:/My%20Documents/CRYPTO%20TOOL/NEW%20EPCRYPTO/EXAMPLE/Option2Exampl
2017-06-22 12:12:30 ERROR validationDetailsLogger:142 - Validation Result: ERROR. Unable to validate H:\My Documents\CRYPTO TOOL\NEW EPCRYPTO\EXAMPLE\Option2Example1.xml
2017-06-22 12:12:30 INFO  validationDetailsLogger:148 - [============ VALIDATION PROCESS AGAINST OFFICIAL EXCHANGE SCHEMA FINISHED ============]
```

Figure 21 EPCryptoToolRequiredDataDetails.log contains error data

3.3.1.1 Example 1 (electoral type and Name missing)

In this log, you will find a description of the Validation ERROR(in below example in which expected electoral type and Name was not provided):

```
2017-06-23 12:57:50 INFO  validationDetailsLogger:103 - [============ VALIDATION
PROCESS OF FILE H:\My Documents\CRYPTO TOOL\NEW
EPCRYPTO\EXAMPLE\Option2Example1.xml AGAINST OFFICIAL EXCHANGE
SCHEMA STARTED: Fri Jun 23 12:57:50 CEST 2017 ============]

2017-06-23 12:57:50 INFO  validationDetailsLogger:126 - Validating H:\My
Documents\CRYPTO TOOL\NEW EPCRYPTO\EXAMPLE\Option2Example1.xml against
XSDs /ep-election-exchange-v1.2.xsd...

2017-06-23 12:57:50 INFO  validationDetailsLogger:127 - List of detailed errors detected during
the Validation Process (if any):

2017-06-23 12:57:50 ERROR validationDetailsLogger:60 - org.xml.sax.SAXParseException;
systemId:
file:/H:/My%20Documents/CRYPTO%20TOOL/NEW%20EPCRYPTO/EXAMPLE/Option2E
xample1.xml; lineNumber: 4; columnNumber: 38; cvc-complex-type.2.4.a: Invalid content was
found starting with element '{"urn:eu:europa:ec:just:epelections:v1":rollEntryList}'. One of
'{"urn:eu:europa:ec:just:epelections:v1":electoralFileType}' is expected.

2017-06-23 12:57:50 ERROR validationDetailsLogger:60 - org.xml.sax.SAXParseException;
systemId:
file:/H:/My%20Documents/CRYPTO%20TOOL/NEW%20EPCRYPTO/EXAMPLE/Option2E
xample1.xml; lineNumber: 7; columnNumber: 16; cvc-complex-type.2.4.a: Invalid content was
found starting with element '{"urn:eu:europa:ec:just:epelections:v1":voter}'. One of
'{"urn:eu:europa:ec:just:epelections:v1":familyName}' is expected.`

2017-06-23 12:57:50 ERROR validationDetailsLogger:142 - Validation Result: ERROR. Unable
to validate H:\My Documents\CRYPTO TOOL\NEW
EPCRYPTO\EXAMPLE\Option2Example1.xml against XSD /ep-election-exchange-v1.2.xsd

2017-06-23 12:57:50 INFO  validationDetailsLogger:148 - [============ VALIDATION
PROCESS AGAINST OFFICIAL EXCHANGE SCHEMA FINISHED ============]
```

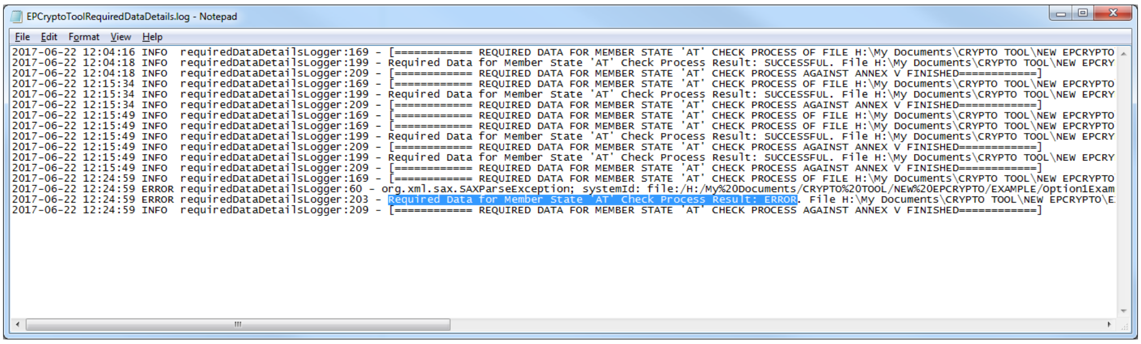
3.3.1.2 Example 2 (In this case we have lack of required date of birth)

```
2017-06-22 12:24:59 INFO  requiredDataDetailsLogger:169 - [============ REQUIRED
DATA FOR MEMBER STATE 'AT' CHECK PROCESS OF FILE H:\My Documents\CRYPTO
TOOL\NEW EPCRYPTO\EXAMPLE\Option1Example1 - Copy.xml AGAINST ANNEX V
STARTED: Thu Jun 22 12:24:59 CEST 2017 ============]

2017-06-22 12:24:59 ERROR requiredDataDetailsLogger:60 - org.xml.sax.SAXParseException;
systemId:
file:/H:/My%20Documents/CRYPTO%20TOOL/NEW%20EPCRYPTO/EXAMPLE/Option1E
xample1%20-%20Copy.xml; lineNumber: 12; columnNumber: 25; cvc-complex-
type.2.4.a: Invalid content was found starting with element
'{"urn:eu:europa:ec:just:epelections:v1":countryOfBirth}'. One of
'{"urn:eu:europa:ec:just:epelections:v1":dateOfBirth}' is expected.

2017-06-22 12:24:59 ERROR requiredDataDetailsLogger:203 - Required Data for Member State
'AT' Check Process Result: ERROR. File H:\My Documents\CRYPTO TOOL\NEW
EPCRYPTO\EXAMPLE\Option1Example1 - Copy.xml is missing required data

2017-06-22 12:24:59 INFO  requiredDataDetailsLogger:209 - [============ REQUIRED
DATA FOR MEMBER STATE 'AT' CHECK PROCESS AGAINST ANNEX V
FINISHED============
```



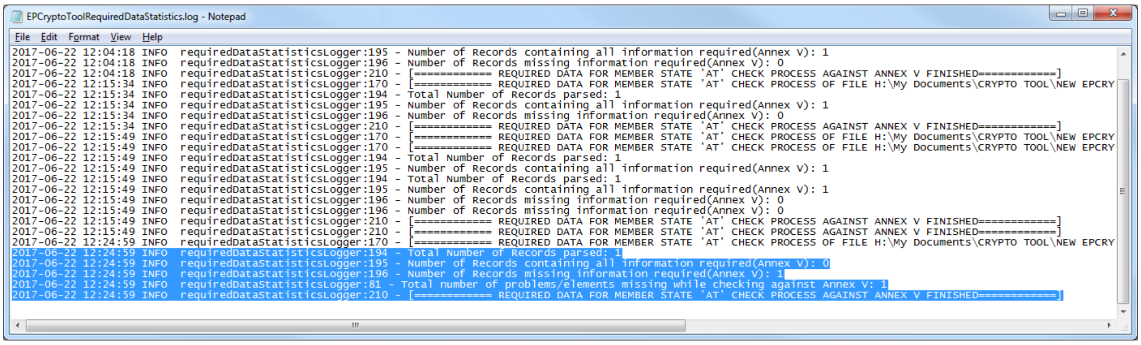
EPCryptoToolRequiredDataDetails.log - Notepad
File Edit Format View Help

```
2017-06-22 12:04:16 INFO  requiredDataDetailsLogger:169 - [============ REQUIRED DATA FOR MEMBER STATE 'AT' CHECK PROCESS OF FILE H:\My Documents\CRYPTO TOOL\NEW EPCRYPTO
2017-06-22 12:04:18 INFO  requiredDataDetailsLogger:199 - Required Data for Member State 'AT' Check Process Result: SUCCESSFUL. File H:\My Documents\CRYPTO TOOL\NEW EPCRY
2017-06-22 12:04:18 INFO  requiredDataDetailsLogger:209 - [============ REQUIRED DATA FOR MEMBER STATE 'AT' CHECK PROCESS AGAINST ANNEX V FINISHED===========]
2017-06-22 12:15:34 INFO  requiredDataDetailsLogger:169 - [============ REQUIRED DATA FOR MEMBER STATE 'AT' CHECK PROCESS OF FILE H:\My Documents\CRYPTO TOOL\NEW EPCRYPTO
2017-06-22 12:15:34 INFO  requiredDataDetailsLogger:199 - Required Data for Member State 'AT' Check Process Result: SUCCESSFUL. File H:\My Documents\CRYPTO TOOL\NEW EPCRY
2017-06-22 12:15:34 INFO  requiredDataDetailsLogger:209 - [============ REQUIRED DATA FOR MEMBER STATE 'AT' CHECK PROCESS AGAINST ANNEX V FINISHED===========]
2017-06-22 12:15:49 INFO  requiredDataDetailsLogger:169 - [============ REQUIRED DATA FOR MEMBER STATE 'AT' CHECK PROCESS OF FILE H:\My Documents\CRYPTO TOOL\NEW EPCRYPTO
2017-06-22 12:15:49 INFO  requiredDataDetailsLogger:169 - [============ REQUIRED DATA FOR MEMBER STATE 'AT' CHECK PROCESS OF FILE H:\My Documents\CRYPTO TOOL\NEW EPCRYPTO
2017-06-22 12:15:49 INFO  requiredDataDetailsLogger:199 - Required Data for Member State 'AT' Check Process Result: SUCCESSFUL. File H:\My Documents\CRYPTO TOOL\NEW EPCRY
2017-06-22 12:15:49 INFO  requiredDataDetailsLogger:209 - [============ REQUIRED DATA FOR MEMBER STATE 'AT' CHECK PROCESS AGAINST ANNEX V FINISHED===========]
2017-06-22 12:15:49 INFO  requiredDataDetailsLogger:199 - Required Data for Member State 'AT' Check Process Result: SUCCESSFUL. File H:\My Documents\CRYPTO TOOL\NEW EPCRY
2017-06-22 12:15:49 INFO  requiredDataDetailsLogger:209 - [============ REQUIRED DATA FOR MEMBER STATE 'AT' CHECK PROCESS AGAINST ANNEX V FINISHED===========]
2017-06-22 12:24:59 INFO  requiredDataDetailsLogger:169 - [============ REQUIRED DATA FOR MEMBER STATE 'AT' CHECK PROCESS OF FILE H:\My Documents\CRYPTO TOOL\NEW EPCRYPTO
2017-06-22 12:24:59 ERROR requiredDataDetailsLogger:60 - org.xml.sax.SAXParseException; systemId: file:/H:/My%20Documents/CRYPTO%20TOOL/NEW%20EPCRYPTO/EXAMPLE/Option1Exam
2017-06-22 12:24:59 ERROR requiredDataDetailsLogger:203 - Required Data for Member State 'AT' Check Process Result: ERROR. File H:\My Documents\CRYPTO TOOL\NEW EPCRYPTO\E
2017-06-22 12:24:59 INFO  requiredDataDetailsLogger:209 - [============ REQUIRED DATA FOR MEMBER STATE 'AT' CHECK PROCESS AGAINST ANNEX V FINISHED===========]
```

Figure 22 EPCryptoToolRequiredDataDetails.log with errors

3.3.2 EPCryptoToolRequiredDataStatistics.log

This log file contains data validation against Annex V statistics on data validated and number of errors found.



EPCryptoToolRequiredDataStatistics.log - Notepad
File Edit Format View Help

```
2017-06-22 12:04:18 INFO  requiredDataStatisticsLogger:195 - Number of Records containing all information required(Annex V): 1
2017-06-22 12:04:18 INFO  requiredDataStatisticsLogger:196 - Number of Records missing information required(Annex V): 0
2017-06-22 12:04:18 INFO  requiredDataStatisticsLogger:210 - [============ REQUIRED DATA FOR MEMBER STATE 'AT' CHECK PROCESS AGAINST ANNEX V FINISHED===========]
2017-06-22 12:15:34 INFO  requiredDataStatisticsLogger:170 - [============ REQUIRED DATA FOR MEMBER STATE 'AT' CHECK PROCESS OF FILE H:\My Documents\CRYPTO TOOL\NEW EPCRY
2017-06-22 12:15:34 INFO  requiredDataStatisticsLogger:194 - Total Number of Records parsed: 1
2017-06-22 12:15:34 INFO  requiredDataStatisticsLogger:195 - Number of Records containing all information required(Annex V): 1
2017-06-22 12:15:34 INFO  requiredDataStatisticsLogger:196 - Number of Records missing information required(Annex V): 0
2017-06-22 12:15:34 INFO  requiredDataStatisticsLogger:210 - [============ REQUIRED DATA FOR MEMBER STATE 'AT' CHECK PROCESS AGAINST ANNEX V FINISHED===========]
2017-06-22 12:15:49 INFO  requiredDataStatisticsLogger:170 - [============ REQUIRED DATA FOR MEMBER STATE 'AT' CHECK PROCESS OF FILE H:\My Documents\CRYPTO TOOL\NEW EPCRY
2017-06-22 12:15:49 INFO  requiredDataStatisticsLogger:170 - [============ REQUIRED DATA FOR MEMBER STATE 'AT' CHECK PROCESS OF FILE H:\My Documents\CRYPTO TOOL\NEW EPCRY
2017-06-22 12:15:49 INFO  requiredDataStatisticsLogger:194 - Total Number of Records parsed: 1
2017-06-22 12:15:49 INFO  requiredDataStatisticsLogger:195 - Number of Records containing all information required(Annex V): 1
2017-06-22 12:15:49 INFO  requiredDataStatisticsLogger:194 - Total Number of Records parsed: 1
2017-06-22 12:15:49 INFO  requiredDataStatisticsLogger:195 - Number of Records containing all information required(Annex V): 1
2017-06-22 12:15:49 INFO  requiredDataStatisticsLogger:196 - Number of Records missing information required(Annex V): 0
2017-06-22 12:15:49 INFO  requiredDataStatisticsLogger:196 - Number of Records missing information required(Annex V): 0
2017-06-22 12:15:49 INFO  requiredDataStatisticsLogger:210 - [============ REQUIRED DATA FOR MEMBER STATE 'AT' CHECK PROCESS AGAINST ANNEX V FINISHED===========]
2017-06-22 12:15:49 INFO  requiredDataStatisticsLogger:210 - [============ REQUIRED DATA FOR MEMBER STATE 'AT' CHECK PROCESS AGAINST ANNEX V FINISHED===========]
2017-06-22 12:24:59 INFO  requiredDataStatisticsLogger:170 - [============ REQUIRED DATA FOR MEMBER STATE 'AT' CHECK PROCESS OF FILE H:\My Documents\CRYPTO TOOL\NEW EPCRY
2017-06-22 12:24:59 INFO  requiredDataStatisticsLogger:194 - Total Number of Records parsed: 1
2017-06-22 12:24:59 INFO  requiredDataStatisticsLogger:195 - Number of Records containing all information required(Annex V): 0
2017-06-22 12:24:59 INFO  requiredDataStatisticsLogger:196 - Number of Records missing information required(Annex V): 1
2017-06-22 12:24:59 INFO  requiredDataStatisticsLogger:81 - Total number of problems/elements missing while checking against Annex V: 1
2017-06-22 12:24:59 INFO  requiredDataStatisticsLogger:210 - [============ REQUIRED DATA FOR MEMBER STATE 'AT' CHECK PROCESS AGAINST ANNEX V FINISHED===========]
```

Figure 23 EPCryptoToolRequiredDataStatistics.log with errors

3.3.3 EPCryptoToolApplication.log

General log file of the application

4 ERROR LOG

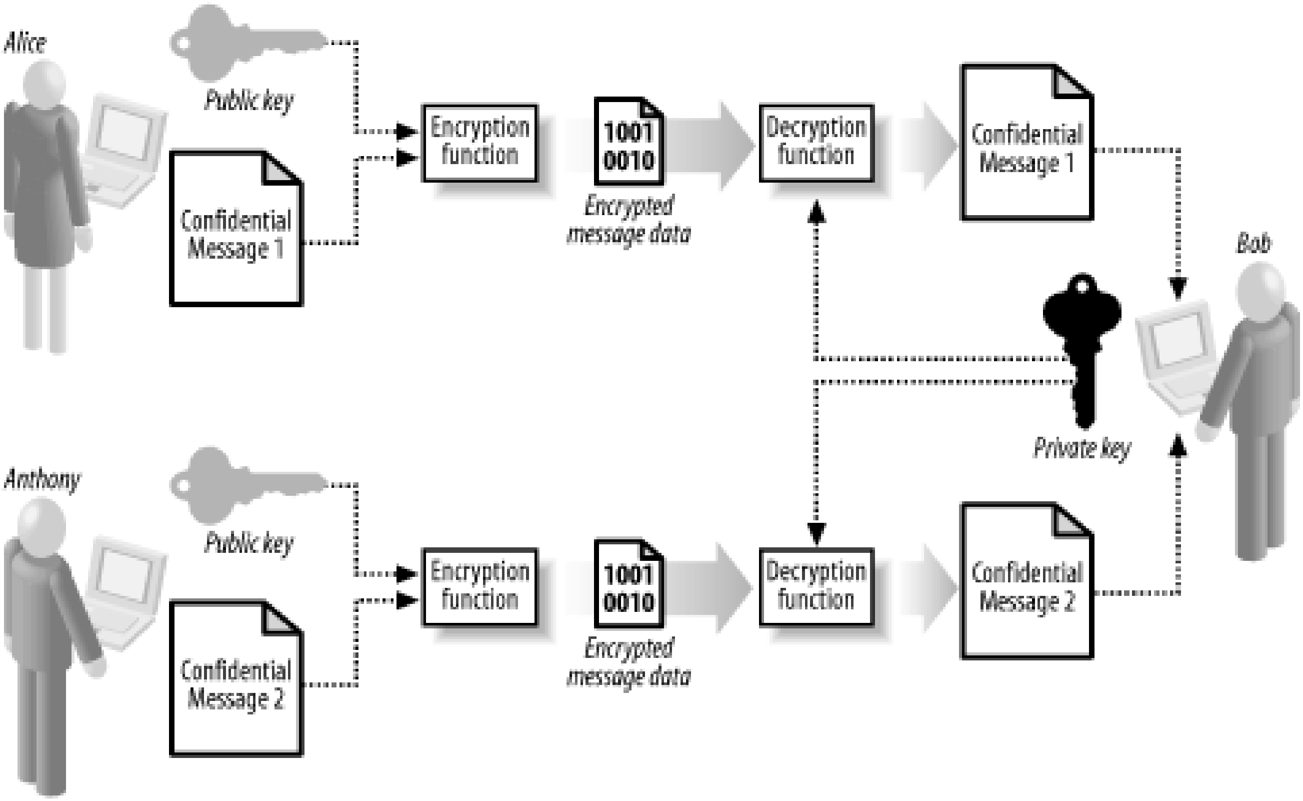
If you encounter any problems using the crypto tool please send to DIGIT-ECI@ec.europa.eu the description of your problem accompanied with the log file EPCryptoToolApplication.log that is stored in the logs subfolder of your crypto tool installation folder.

5 APPENDIX A: CRYPTOGRAPHY & BEST PRACTICES

Cryptographic method description

EP crypto tool is using public-key encryption (also called asymmetric encryption) for the encryption of the data to be transferred between Member States[1]. This involves a pair of keys for each Member State, a public key (known in this document as 'credentials') and a private key that is handled by the software transparently and without user intervention. Each public key is meant to be published, and the corresponding private key is meant to be kept secret.

Data encrypted with a public key can be decrypted only with the corresponding private key. The scheme allows public keys to be freely distributed, while only authorised people are able to read data encrypted using this key. In general, to send encrypted data, the data is encrypted with that person's public key, and the person receiving the encrypted data decrypts it with the corresponding private key.



For more details: Asymmetric Encryption Explained

- Other encryption parameters:

[1] More accurately, the European Parliament cryptographic tool uses a hybrid mechanism: A symmetric AES 256 key is used to (d)encrypt the original file and the couple of RSA asymmetric public/private keys are used to (d)encrypt the symmetric key. The handling of the symmetric key is done by the application and is transparent for the user.

- AES 256 to encrypt the data (symmetric encryption)
- The size of the Asymmetric key is 4096
- RSA with an Optimal Asymmetric Encryption Padding to encrypt the AES key (password protected) and to sign the encrypted content ((cypher: RSA/ECB/OAEPWithSHA-512AndMGF1Padding)
- The hashing functions are performed with SHA512
- The number of iteration for the password hashing is 64000.
- Maximum period of validity of the encryption key:

  Responsibility of the Member States
- Minimum requirements for the password:

  Minimum 10 characters
  A least one special character
  A least one number
  Upper case and lower case characters

6 APPENDIX B: BEST PRACTICES FOR HANDLING THE KEYS

The public keys ('credentials') uploaded by Member States to the File Exchange Service are not confidential and can be transferred just like any other file (via email or a repository such as S-CircaBC). There is no confidentiality issue if all Member States' credentials are shared in a common repository.

The handling of the private asymmetric key is done transparently by the application and this key, although confidential, is never exposed. The private keys are stored in the folder of the application. It is then important that those folders are not publicly available. The password to access the credentials should only be communicated via secured communication.

If the keys are lost, the Member State can either:

a. Restore its public key if it took a back (refer to §2.7)
b. Generate new keys and re-encrypt the data. In this case, the user is informed by the tool that the new credential must be shared with the Commission (DIGIT-ECI@ec.europa.eu)