Council of the
European Union

Brussels, 17 January 2018
(OR. en)

5202/1/18
REV 1

MIGR 1
COMIX 3

'I/A' ITEM NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee/Council
Subject:	Irregular Migration Management Application (IRMA) - Technical guidelines for Return Operational Data Collection - Encryption of Exchanged Files = Endorsement

1. The European Commission has developed IRMA (Irregular Migration Management Application), a restricted information system. IRMA is a secure electronic platform which connects Member States and Schengen Associated States (further referred to as IRMA Countries), the European Commission (DG HOME), the European Border and Coast Guard Agency (EBCGA) and the relevant EU funded programmes at operational, practitioner level in order to build synergies and to enable work in a mutually reinforcing way. To further support Member States in the implementation of return the following two guidelines have been developed at technical level in full consultation with them: **Return Operational Data Collection** and a **Data Encryption Scheme.**

   The **Return Operational Data Collection** component is designed to provide a close-to-real-time overview of the operational situation in the area of return in order to facilitate the management and return of irregular migrants at EU level. Such a reporting takes place on a voluntary basis.

The **Data Encryption Scheme** provides IRMA with the means to be able to support the encryption of files that are exchanged among its users on a voluntary basis whenever this is deemed necessary by the users themselves, for example in relation to Data Protection.

2. The text of the draft **IRMA Return Operational Data Collection** and of the **IRMA Data Encryption Scheme** was considered by the Integration, Migration and Expulsion Working Party (Expulsion) at its meetings on 6 October and 6 December 2017 and agreed by delegations.

3. The Permanent Representatives Committee and the Council are invited to endorse the attached **IRMA Return Operational Data Collection** and **IRMA Data Encryption Scheme**.

ANNEX I

TECHNICAL GUIDELINES FOR RETURN OPERATIONAL DATA COLLECTION

INTRODUCTION

The restricted information exchange system developed by the European Commission, named **Irregular Migration Management Application (IRMA)** is a secure electronic platform which connects Member States and Schengen States (further referred to as IRMA Countries), the European Commission (DG HOME), the European Board and Coast Guard Agency (EBCGA) and the relevant EU funded programmes at operational, practitioner level in order to build synergies and to enable work in a mutually reinforcing way.

The Operational Data Collection component is designed to provide a close-to-real-time overview of the operational situation in the area of return in order to facilitate the management and return of irregular migrants at EU level. Such a reporting takes place on a voluntary basis. Thanks to the operational return data collection, Member States, the Commission and the EBCGA will be quickly able to identify and analyse return implementation challenges. Further added value in collecting the operational return data lies in the fact that IRMA, through its "IRMA Request" module will allow MS but also Commission or EBCGA to "trigger" specific return support measures/actions initiated by the relevant responsible stakeholder i.e. the Commission the EBCGA, one of the EU funded return projects or through pre-arranged individual contractual arrangements with specific service providers using the standalone AMI system. Such requests could for example include planning of resources for specific return activities including information campaigns, the launch of joint return actions, shared management of consular cooperation on requests for readmission, identification and travel documents, the organisation of identification missions, requests for specific support by third country based liaison officers, shared use of facilities, identification of specific funding needs, launching of pilot actions, common procurement arrangements with AVR(R) service providers, benchmarking to promote and improve best practices among Member States etc.

It will also be instrumental in evaluating the level of cooperation on readmission and return of third countries and the resulting adaptation of our position and actions towards them. Needless to say that the interpretation of the data collected and specific measures taken on that basis will always be decided with the involvement of all parties concerned during meetings like the monthly Readmission Experts Meetings, the quarterly European Migration Network – Return Experts Group Meetings or the EBCGA DCP meetings and any other ad hoc meeting organised for this specific purpose.

The objective of these guidelines is to present the general framework of the Operational Data Collection, as well as explain the relevant indicators, units of measure and disaggregations. Technical information concerning the detailed workflow of the Operational Data Collection will be specified in the User Manual.

The objective of the Operational Data collection is twofold:

a. Collecting and recording of the Operational Data for the internal purposes and activities of each IRMA Country;

b. Making the Operational Data available to the clearly defined, restricted group of Operational Data Report Accessors, comprising selected representatives of DG HOME, the EBCGA, EASO and from IRMA Countries according to the specified dissemination scheme.

Operational Data collected via IRMA differs from official statistical data published by Eurostat, which are subject to a stricter quality control. Some of the indicators refer to the Eurostat methodology (with the corresponding tables), however due to the processing time constraints with regard to making Operational Data available to the restricted group of IRMA users, there will be an inherent margin of error in the data, resulting in limitations in the comparability of Operational Data with Eurostat statistics. This margin of error should be mitigated to an extent by the possibility of continuous data collection, compilation and revision in the course of a calendar year within the country-wide level of the database in order to account for data e.g. from external sources, such as organisations implementing assisted voluntary departure programs.

IRMA Countries are responsible for ensuring data collection from all relevant national authorities.

The process of ongoing coordination between DG HOME (IRMA), Eurostat, the EBCGA and EASO has been put in place in the form of Working Group on Quality Statistics, launched on 26th January 2017. The objectives of this working group include ensuring coherence between IRMA indicators and the Technical Guidelines for the Enforcement of Immigration Legislation (EIL) data collection.

DATABASE ARCHITECTURE

The Operational Data of each IRMA Country will be first recorded and consolidated at the country-wide level, and consequently made available to the restricted database of the IRMA community. The data collection tool supports two sub-features, which will be clearly separated (accessible by separate links allowing parallel viewing of the two features) and subject to separate distinct workflows:

a. ***Data Collection***[1] ***(country-wide database)*** for the collection, recording and management of Operational Data in the Country-wide database.

b. ***Data Publishing (restricted IRMA database)*** for publishing of the Operational Data that have already been collected at Country-wide Dissemination Level in the restricted IRMA database.

[1] Titles tbc following the completion of the tool development

Data Collection (country-wide database)

Operational Data of each IRMA Country will be collected independently and on a voluntary basis and managed within the Country's own restricted IRMA Workspace, accessible only to IRMA users from the specific IRMA Country. The data collection tool will be accessible exclusively to persons from relevant national authorities authorised to contribute to the data collection, as well as to consolidate and publish it. Two categories of user rights will be created for this purpose: ***Data Collectors***, authorised to create draft data collections serving as contributions of their respective authorities to the country-wide data collection, and ***Data Submitters***, who will also be authorised to consolidate draft data collections and making the final collection available to the limited group of Operational Data Report Accessors within the restricted IRMA database.

At national level, the database supports online collaboration of multiple users from individual national authorities who can simultaneously save drafts containing their contributions, which will consequently be subject to compilation and validation by the Data Submitter before publishing in the IRMA-wide database.

Data input for a reference month will be available as of the first day of the reference month. As soon as a draft contribution is added, it will become visible to all other data contributors and submitters of a given IRMA Country.

Contributions will be prepared by Data Collectors, consolidated by the authorised Data Submitter and submitted to the IRMA database **by 30th calendar day of the month following the end of the reference month**. That means that the monthly data collections relating to month M are drafted by Data Collectors and consolidated by Data Submitters by the 30th day of month M+1. Given these limitations and the fact that certain data may only become available after the prescribed deadline, monthly data will be treated as provisional, presenting a snapshot of the situation at the time of recording. Only final annual data collection will provide a final overview of the data collected during the year.

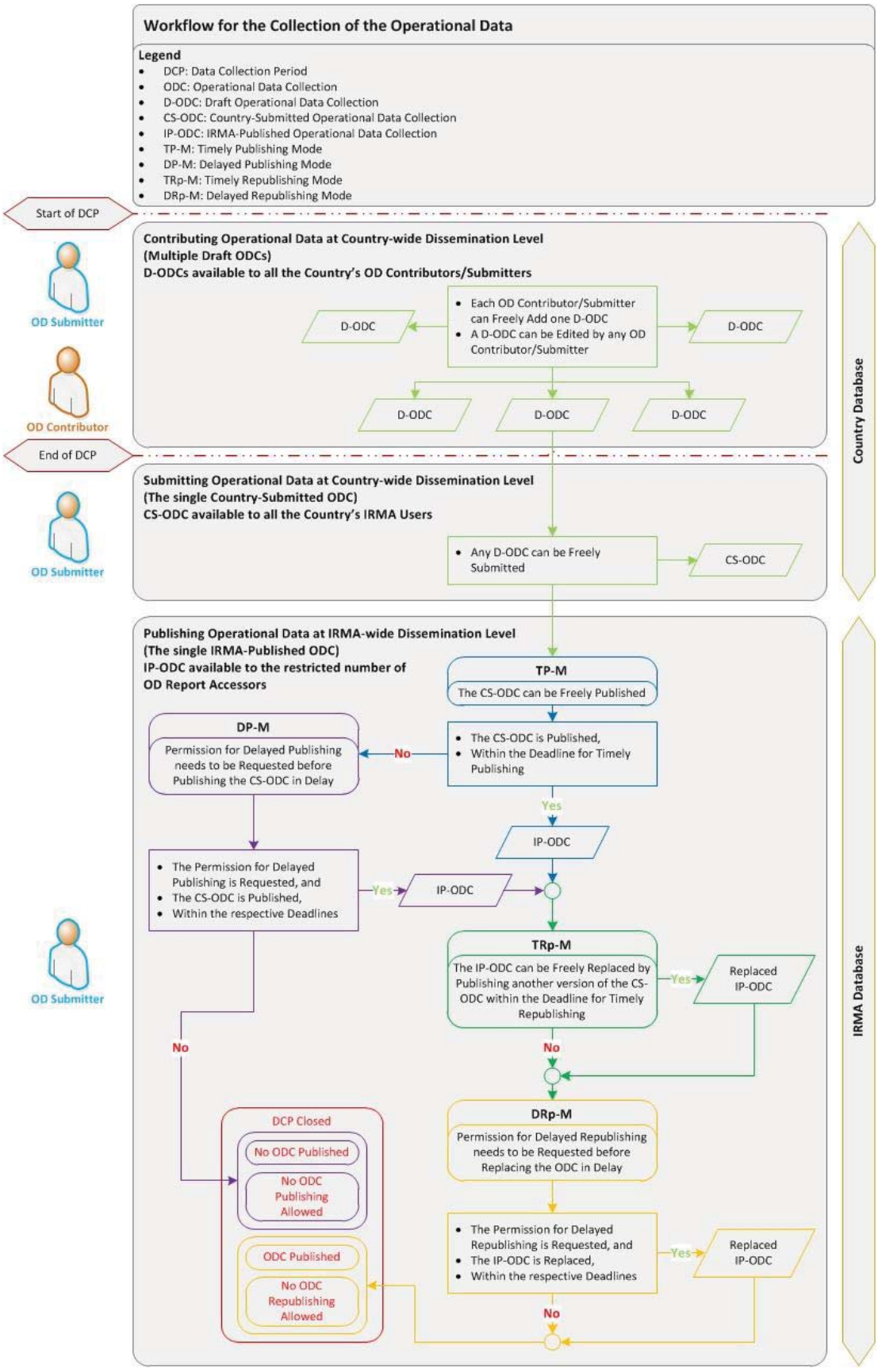
The system will allow inputting numerical values (non-negative integers) or non-numerical values: **'N/Av'** to signify **'Data not available'** (meaning: data for this indicator is in principle recorded/collected but is unavailable e.g. for technical reasons) and **'N/Ap'** to signify **'not applicable'** (data for this indicator/disaggregation is not collected or the Member State cannot provide this dataset at IRMA-wide level). Data sources to be used in the reporting will be the same as for the Eurostat data collections contributions. The Data Collection will be accompanied by a monthly Data Accuracy Assessment sheet, which will enable providing qualification of and explanation for the level of accuracy of the provided data. **Justifications (in English) are obligatory for indicators where non-numerical values are provided.**

Until this deadline, Data Collectors in IRMA Countries can modify and save their data without limitations (subject to the internal deadline established by the national Data Submitters to allow for data compilation). It is only when data is published via the dedicated data publishing feature (and the button "Publish" is pressed) that the data is transferred to the restricted IRMA database and becomes accessible to the limited number of Operational Data Report Accessors.

The country-wide collection level allows revision of data without limitations during the entire annual collection timescale, i.e. by 31 March of the year Y+1 with view to facilitating data collection and revision for the purpose of preparing contributions for the Eurostat annual data collection. Revision of final annual data will be possible upon request to allow the possibility of aligning the figures with any possible corrections and revisions made in the data provided to Eurostat.

Data Publishing (restricted IRMA database)

Each IRMA Country will make its Country-wide compilations of Operational Data counts available to the restricted community of Operational Data Report Accessors authorised to view the data of all IRMA Countries with the use of a dedicated reporting tool. The publishing of the Country-wide Operational Data in the restricted IRMA database (statistical database) will be performed by the Data Submitters, authorised to compile and publish data in accordance with the following data collection flowchart.



DATA COLLECTION FRAMEWORK

Periodicity

Two complementary timescales of data collection will be used:

a) **monthly** – reference periods will correspond to (Gregorian) calendar months.

b) **annual** – calendar year, enabling comparison between data made available to the restricted IRMA community with data collected continuously in the country-wide database level, as well as submission of completed and validated annual data to the restricted IRMA community.

The first reference period for data collection is January 2017.

Data submission to the IRMA Dissemination Level

For monthly data:

Data compiled at the Country-wide level of the database is published in the restricted IRMA-wide database level by the 30th day of the month following the end of the reference month.
In case the deadline for publishing data is not respected, an automatic alert will be generated and sent to every person in the given IRMA country responsible for submitting Operational Data to the restricted IRMA database, as well as to the General Manager of their respective national authority. A corresponding notification will be also sent to the Commission to enable it taking necessary actions, such as taking contact with the relevant responsible persons. This procedure applies to all reference periods.

Should a revision of data for the reference month be necessary, IRMA Countries can request to revise data once during a period of two weeks following the data publishing deadline or, if later, with some justification. The key purpose of the requirement to request revision is to notify the Commission that such a revision has taken place (necessary for the purpose of reporting).

This workflow does not affect the free editing possibility of data within the Country-wide database throughout the entire reference year. Nevertheless, monthly data will be treated as provisional, presenting a snapshot of the situation at the time of recording. Only final annual data collection will provide a final overview of the data collected during the year.

For annual data collection:

Within three months of the end of the reference year, i.e. the first annual data relating to the year Y are expected by 31 March of the year Y+1, at the latest. Revision of final annual data will be possible upon request to allow the possibility of aligning the figures with any possible corrections and revisions made in the data provided to Eurostat.

Acces to and use of the data at IRMA-wide level

The data at IRMA-wide level is restricted and can only be used for internal purposesand activities. None of the data is allowed to be published.
All the Operational Data Users who are designated to access the data at IRMA-wide level, have to sign the Operational Data User Charter (see Annex 1) before. All users having access to the data at IRMA-wide level are listed in IRMA with a copy of their signed User Charter.

Data format:

Data Collectors from individual organisational entities will have the possibility of either entering data in the national workspace of IRMA for the purposes of compilation by the Data Submitter at national level either via the dedicated web form (manual editing, including copy/paste facility), either by uploading the predefined CSV file or XML file. Compilation of data submitted in this manner by Data Collectors and validation before publishing in the restricted IRMA database will be performed by Data Submitters via the dedicated web form.

Subject:

The requested Operational Data relate to **third country nationals issued a return decision** only. The term "third country national" is defined by the Return Directive[2] as "any person who is not a citizen of the Union within the meaning of Article 20(1) of the Treaty on the Functioning of the European Union and who is not a person enjoying the right of free movement under Union law as defined in Article 2(5) of the Schengen Borders Code[3], including stateless persons." Furthermore, as defined in the Return Handbook[4], the following categories of persons are not considered "third-country nationals":

- Persons who are Union citizens within the meaning of Article 20(1) TFEU (previously Article 17(1) of the Treaty) = persons holding the nationality of an EU Member State2;
- Persons holding the nationality of EEA/CH;
- Family members of Union citizens exercising their right to free movement under Article 21 TFEU or Directive 2004/38/EC;
- Family members of nationals of EEA/CH enjoying rights of free movement equivalent to Union citizens.

Any other person (including a stateless person) is to be considered "third-country national".

---

2 Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals, OJ L 348 of 24.12.2008, p. 98.

3 Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (codification), OJ L 77, 23.3.2016, p. 1.

4 Annex 1 of Commission Recommendation C(2015)6250 final of 01/10/2015 establishing a common "return handbook" to be used by Members States' competent authorities when carrying out return related tasks.

Unit of measure

The unit of measure of each dataset is the absolute **number of persons per return procedure**, not the number of administrative decisions or acts.

In the majority of datasets the figure requested is the total number of persons to whom e.g. decisions were issued or with regard to whom requests were made / replies or documents were received during the reference month. In cases where one return decision is issued or a readmission application is made for several persons (e.g. a family), it is the number of persons that will be recorded.

Datasets collected within the IRMA Operational Data collection are divided into two categories:

- **Flow data**, measured over an interval of time, i.e. the reference month.
  With regard to indicators 1, 4a, 4b, 5b, 5c, 5d, 5e, 5g, 6, 7, 8 each person will be counted only once. Given the difficulty concerning accounting for repeated decisions issued or returns performed during the course of the year in data provided on a monthly basis, a margin of error will be accepted with regard to operational monthly data. Data provided on the annual basis, however, will be corrected to avoid double-counting of persons in order to guarantee the accuracy and comparability of the data.

- **Stock data**, measured at a particular point in time, representing a quantity existing at that point in time, i.e. the last day of the reference month.
  With regard to datasets 2a, 2b, 3, 5a, 5f each person will be counted once only at the end of the reference month, however the same person may be included in the dataset repeatedly over a period of several (consecutive) months. Since these indicators refer to stock numbers of persons (e.g. in detention), the figures will not be added up in the IRMA-level data reporting (in case quarterly or annual aggregations are extracted in the reporting tool, only average will be automatically calculated by the system).

Definitions of disaggregations:

Citizenship

All datasets will be collected per citizenship (or nationality) of third country nationals subject to return. In the case of a third country national with more than one citizenship or a family with different citizenships among family members, the citizenship corresponding to the country of intended return (in case it is the country of origin of at least one family member and not a transit country) should be taken into account. Depending on the stage of the procedure, citizenship may be given, as stated by the third country national, or verified, e.g. in the process of identification/readmission procedure or another procedure (e.g. asylum application).

Gender

The basis for recording gender in the datasets is the gender accepted by the recording national authority (whether authority responsible for return or asylum authority).

Age

The basis for recording ages in the datasets is the age accepted by the recording national authority (whether authority responsible for return or asylum authority). It may be the age claimed by the person and accepted by the authorities or the age determined by the competent asylum authorities. Please note that in case a national authority carries out an age assessment procedure in relation to the returnee claiming to be a minor, the age reported in this table shall be the age determined by **the age assessment procedure**[5].

[5] Where the age assessment procedure assigns an age range to the person and the asylum authority takes into account the lowest point of that range, that point should be reported.

The age recorded by authorities will relate to the **age at the date of the administrative event** i.e. for persons issued return decisions it will be the age recorded at the point of issuing the decision. For stock data (indicators 2a, b, 3), the age should be that of the person at the end of the reference period. The two disaggregations by age group ('14 years and under' and '15-17 years old'), as well as and 'Number of unaccompanied minors' are subsets of the 'Number of minors' disaggregations. The two age group subsets should sum up to provide a total (overall total, M, F respectively) indicated in the 'Number of minors' disaggregation.

Age categories collected will cover minors (under 18 years old) and unaccompanied minors. **Unaccompanied minors** means minors as defined in Article 2(k) and (l) of Directive 2011/95/EU that is "third-country nationals or stateless persons below the age of 18, who arrive on the territory of the Member States unaccompanied by an adult responsible for them whether by law or custom, and for as long as they are not effectively taken into the care of such a person; it includes minors who are left unaccompanied after they have entered the territory of the Member States.". The 'Number of unaccompanied minors' disaggregation, while a subset of the 'Number of minors' dataset, should be treated separately from the age group disaggregations, i.e. unaccompanied minors should be recorded in the respective age group, as well as separately in the unaccompanied minors subset.

The age of unaccompanied minors reported in this table shall refer to the age accepted by the national authority. In case the responsible national authority carries out an age assessment procedure in relation to the applicant claiming to be an unaccompanied minor, the age reported in this table shall be the age determined by the age assessment procedure.
In cases where persons initially registered as minors (e.g. in datasets 1, 2) reach the age of 18, they will be further recorded as adults e.g. in datasets concerning pre-return procedures and effective returns, even if that were to result in some discrepancies of data.

Forced returns, assisted voluntary departures and unassisted voluntary departures

Indicators 4a and 4b are additionally disaggregated by: **forced returns**, ass**isted voluntary departures** and **unassisted voluntary departures**, where these are reliably recorded.

Forced return should be understood as removal in the meaning of Article 3(5) of the Return Directive, i.e. the enforcement of the obligation to return, namely the physical transportation out of the Member State is a specific form of compulsory (forced) return.

Assisted voluntary departure should be understood as voluntary departures in the meaning of the Return Directive, i.e. voluntary compliance with an obligation to return of illegally staying third country nationals, supported by logistical, financial and/or other material assistance. Where no distinction is recorded between assisted voluntary departures of holders of return decisions and assisted voluntary returns of other third country nationals, this dataset will cover both groups.

Unassisted voluntary departure should be understood as voluntary departures in the meaning of the Return Directive, undertaken without logistical, financial and/or other material assistance. Unassisted voluntary departures should be calculated where these are reliably recorded. According to the proposal of the EIL Task Force, reliably recorded means that there is official evidence that person left the country voluntarily (e.g. confirmation is provided by the Border Authority). Where no distinction is recorded between voluntary departures of holders of return decisions and other third country nationals, this dataset will cover both groups.

Moving from the national territory of one Member State to the territory of another Member State in accordance with Article 6(2) (see below section 5.4.) cannot be considered as voluntary departure. The definition of voluntary departure always requires departure to a third country. The only exception to this rule is indicator 4b, which has been intentionally aligned with the Eurostat indicator **'Third country nationals who have actually left the territory (art 7(1)(b)) following a decision or an act under art 7(1)(a)'**, which refers to the TOTAL of all persons who have in fact left the national territory of the IRMA country having been previously issued a return decision, and includes both returns in the meaning of Article 3(3) of the Return Directive (dataset 4a) and transfers to other Member States (e.g. passing back of irregular migrants on the basis of a bilateral agreement, as per Article 6(2) of the Return Directive).

Reference area

IRMA Countries, i.e. EU28 Member States, Iceland, Liechtenstein, Norway and Switzerland.

Overview of the datasets (see more detailed explanations below)

1. Persons issued a return decision (flow)

2a. Persons with a return decision in detention (stock)

2b. Persons with a return decision subject to restrictive measures (stock)

3. Persons ready to be returned (with Travel Document + identified + documented + available) (stock)

4a. Persons effectively returned to a third country (flow)

4b. Persons who have effectively left the territory of the IRMA Country (flow)

Identification / Emergency Travel Documents (ETD)

5a. Number of persons with a return decision, needing identification (stock)

5b. Number of persons with verification/identification requests/requests for ETD submitted by MS (flow)

5c. Number of persons identified positively with no ETD issued (flow)

5d. Number of persons with ETD issued (flow)

5e. Number of persons for whom negative replies to the identification request were received

5f. Number of persons with pending replies to the identification requests / no replies received (stock)

5g. Number of identifications performed/travel documents issued within deadline (where applicable) (flow)

6. Number of persons with EU Travel Documents readmitted by the third country (flow)

7. Number of persons whose readmission was refused at the border (flow)

8. Number of persons returned on charter flights (flow)

Go to View Mode | Input Helper | Delete Draft

Brazil (BR) | Switch to Indicator View | Manage Countries

Browse... No file selected.

Import CSV | Export to CSV

	Number of persons				Number of adults (>=18)				Number of minors (<18)				14 years old and under				15-17 years old				Age unknown				Number of unaccompanied minors			
	Total	M	F	?	Total	M	F	?	Total	M	F	?	Total	M	F	?	Total	M	F	?	Total	M	F	?	Total	M	F	?
Persons issued a return decision	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Persons with a return decision in detention (stock)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Persons with a return decision subject to restrictive measures (stock)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Persons not in detention/subject to restrictive measures, but with known whereabouts (stock)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Persons ready to be returned (stock)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Persons effectively returned to a third country																												
forced returns	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
assisted voluntary returns	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
voluntary returns	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Persons who have effectively left the territory of the IRMA Country																												
forced returns	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
assisted voluntary returns	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
voluntary returns	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Identification / Emergency Travel Documents (ETD)	Total
Number of persons with a return decision, needing identification (stock)	0
Number of persons with verification/identification requests/requests for ETD submitted by MS in a given month	0
Number of persons identified positively with no ETD issued	0
Number of persons with ETD issued	0
Number of persons for whom negative replies to the identification request were received	0
Number of persons with pending replies to the identification request / no replies received (stock)	0
Number of persons with identifications performed/travel documents issued within deadline (where applicable)	0
Number of persons with EU Travel Documents readmitted by the third country	0
Number of persons whose readmission was refused at the border	0
Number of persons returned on charter flights	0

Save

INDICATORS

Dataset 1. Persons issued a return decision (flow)

In terms of data subject the dataset corresponds directly to the Eurostat indicator *'Third country nationals, who are subject to an obligation to leave (article 7(1)(a) of Regulation 862/2007)'*. The dataset covers the number of persons issued return decisions during the reference month.

According to Article 6(1) of the Return Directive, a **return decision is** *an **administrative or judicial decision** or act, stating or declaring the stay of a third-country national to be illegal and **imposing or stating an obligation to return**. A return decision may contain elements such as an entry ban, a voluntary departure period, designation of the country of return.* Return decisions can be issued in the form of a self-standing act or decision or together with other decisions, such as a removal order or a decision ending legal stay.

The dataset refers to the number of persons, not to the number of administrative decisions or acts. "Persons issued a return decision" will be recorded when issued the first return decision / decision obliging a given person to leave the territory of Member States. In cases, where a given person receives a return decision more than once during the course of one or several years, that person will be recorded only once, in the first year and in the first month when the initial return decision is issued, provided that the decisions were issued in the course of the same return procedure.

Persons refused entry at the border will not be included in this dataset, except if the refusal is not performed, no authorisation to stay is issued, but the person enters the territory.

If Member States issue return decisions and removal orders in two separate documents and at different moments in time, they should not report removal orders, as these are decisions specifying the manner of return and not imposing the obligation to leave. This recommendation is consistent with the outcome of the EIL Task Force discussions as proposed to the Member States.
The exception would be the consecutive decision issued to a person which has already been effectively returned following a previous decision, but was found to be irregularly staying or applied for asylum and was rejected again. The first decision issued to such a person following return will be taken into account again.

Unit of measure:

- Number of persons;

Disaggregations:

- Citizenship;
- Gender;
- Age;
- Unaccompanied minors.

Dataset 2a. ***Persons with a return decision in detention (stock)***

This dataset refers to the number of persons having been previously issued a return decision, who are placed in detention for return purposes as referred to in Article 15 of the Return Directive. In the EU return context, Member States may only detain or keep in a detention facility a third-country national who is the subject of return procedures in order to prepare the return and/or carry out the removal process, in particular when: (a) there is a risk of absconding; or (b) the third-country national concerned avoids or hampers the preparation of return or the removal process. This dataset will not include persons detained at the border as a result of refusal of entry.

The number of persons issued a return decision that are under custodial measures for purposes other than return (criminal cases), are excluded from this dataset.

The number of persons in detention will be calculated as at the end of the month. The objective of this approach is to exclude from the dataset (or at least limit the reporting of) e.g. short-term (24-48 hours) detentions followed by an immediate release of the returnee. In this dataset each person is counted only once at the end of the reference month, however can be included in the dataset repeatedly over a period of several (consecutive) months.

Unit of measure:

- Number of persons

Disaggregations:

- Citizenship;
- Gender;
- Age;
- Unaccompanied minors.

Dataset 2b. ***Persons with a return decision subject to restrictive measures (stock)***

Restrictive measure refers to any alternative to detention, defined as non-custodial measures used to monitor and / or limit the movement of third-country nationals in advance of compulsory return or deciding on the individual's right to remain in the Member State, such as regular reporting to the authorities, the deposit of a financial guarantee, residence restrictions, the surrender of travel documents, electronic monitoring, placement in a freedom-restricting centre or in a Family Unit. (Derived by EMN from Art. 8(4) of Directive 2013/33/EU Recast Reception Conditions Directive, completed by the IRMA survey in May 2017 and bilateral exchanges with the Member States). This dataset refers to the number of persons having been previously issued a return decision, who are placed under a restrictive measure/alternative to detention, as calculated at the end of the month. In case no restrictive measures are defined in national legislation or applied, this dataset should be qualified as 'Not applicable' and a corresponding explanation provided in the Quality Evaluation sheet.

In this dataset each person is counted only once at the end of the reference month, however can be included in the dataset repeatedly over a period of several (consecutive) months or may be recorded again in case of consecutive detention.

Unit of measure:

- Number of persons

Disaggregations:

- Citizenship;
- Gender;
- Age;
- Unaccompanied minors.

Dataset 2c. ***Persons not in detention and not subject to restrictive measures, but with known whereabouts (flow)***

Given that reliable reporting on persons with known whereabouts is possible only during a limited period of time following verification thereof, it is impossible for Member States to provide stock data.

As the collection of flow data on this dataset presents no added value, it has been decided to remove dataset 2c from the Operational Data Collection.

Dataset 3. ***Persons ready to be returned for whom the removal is not organised (stock)***

This dataset refers to the number of persons, with regard to whom all objective requirements for return have been fulfilled, i.e. are **identified + with a Travel Document or documented + available + no ongoing procedure with suspensive effect on the return decision, but for whom the removal has not yet been organised**.

More specifically, persons in question are in possession of valid travel documents, verified by the national authorities where necessary; in case of persons not in possession of valid travel documents, the procedure of verification of their identity and establishing citizenship has been successfully completed: their citizenship has been confirmed by their national authorities and an Emergency Travel Document has been issued and remains within its validity period or an EU Travel Document has been issued.

Availability of persons in question means that they are either placed in custody or an alternative to detention, or their whereabouts are known to the authorities (with a caveat on the limited reliability of the latter number). In addition, no procedures, with a suspensive effect on the return decision and its implementation, are ongoing.

In this dataset each person is counted only once at the end of the reference month, however the same person can be included in the dataset repeatedly over a period of several (consecutive) months.

This dataset will allow IRMA Countries or the EBCGA to take the initiative for the organisation of joint return operations.

Unit of measure:

- Number of persons

Disaggregations:

- Citizenship;
- Gender;
- Age;
- Unaccompanied minors.

Dataset 4a. Persons effectively returned to a third country

In terms of data subject, this dataset corresponds directly to the Eurostat sub-category *'Third country nationals who have actually left the territory to a third country following a decision or an act under art 7.1.a'*, covering those persons who are recorded as having returned to a third country following an order to leave. This category covers third-country nationals returned to their country of origin, a country of transit in accordance with Community or bilateral readmission agreements or other arrangements or another third country, to which the third-country national concerned voluntarily decides to return and in which he or she will be accepted, excluding EU28 countries, Iceland, Liechtenstein, Norway and Switzerland.

Within the reference period (i.e. month or year for the annual collection), each person should be counted only once per return procedure. Each category refers to the number of persons, not to the number of administrative decisions or acts.

Unit of measure:

- Number of persons

Disaggregations:

- Citizenship;
- Gender;
- Age;
- Unaccompanied minors.
- Forced returns, assisted voluntary departures and unassisted voluntary departures.

Dataset 4b. Persons who have effectively left the territory of the IRMA Country

The dataset corresponds directly with the Eurostat indicator *'Third country nationals who have actually left the territory (art 7(1)(b)) following a decision or an act under art 7(1)(a)'*.

This category refers to the TOTAL of all persons who have in fact left the national territory of the IRMA country having been previously issued a return decision, and **includes both returns in the meaning of Article 3(3) of the Return Directive** (dataset 4a), **as well as transfers to other Member States and intra-Schengen transfers (e.g. passing back of irregular migrants on the basis of a bilateral agreement, as per Article 6(2) of the Return Directive).**

These data do not include persons who are transferred from one Member State to another under the mechanism established by the Dublin Regulation (Council Regulation (EC) No 343/2003 and (EC) No 1560/2003, for these cases see related Dublin Statistics).

Within reference period (i.e. month or year for the annual collection), each person should be counted only once per return procedure. Each category refers to the number of persons, not to the number of administrative decisions or acts.

Unit of measure:

- Number of persons

Disaggregations:

- Citizenship;
- Gender;
- Age;

- Unaccompanied minors.

- Forced returns, assisted voluntary departures and unassisted voluntary departures.

Identification / Travel Documents (TD)[6]

Dataset 5a. ***Number of persons with a return decision, needing identification (stock)***

This dataset refers to the sub-category of persons issued return decisions, whose citizenship has to be confirmed by the authorities of their stated country of origin, as they are not in possession of documents which could serve as a proof of citizenship, such as valid or expired travel documents or identity documents, copies of such documents, birth certificates or copies thereof or residence permits and their copies or any other official documents stating the citizenship of heir holder.

This data is useful in that it enables IRMA Countries, the EBCGA and EURINT to coordinate identification missions.

Dataset 5b. Number of persons with verification/identification requests/requests for TD submitted by MS in a given month (flow)

This dataset refers to the total number of persons with regard to whom during a given reference month requests were submitted to third countries for:

- verification or identification, e.g. including both requests for verification / establishing citizenship based on valid or expired documents or their copies, and requests for identification / establishing citizenship based on interviews by consular or diplomatic authorities, biometric data such as fingerprints or photographs or other data gathered with regard to the person;

- requests for issuing of a Travel Document necessary for the purpose of return;

- readmission requests in accordance with bilateral or EU readmission agreements.

6 Under Travel Document is understood any travel document that allows the person issued a return decision to travel to the third country of return, i.e. an Energy Travel Document, Laissez-passer, Passport, etc.

Since each such request may serve more than one purpose (identification and issuing of a TD), all persons for whom any of such requests has been submitted will be included in this category.

Datasets 5b to 5g will give indication on the level of cooperation of third countries on return and readmission.

Dataset 5c. Number of persons identified positively with no TD issued (flow)

This dataset refers to the number of persons, who were positively identified as citizens of a given country by its central, diplomatic or consular authorities during a given reference month, for whom no Travel Document has been issued yet or with regard to whom the diplomatic or consular authorities refused to issue a Travel Document despite a positive identification.

Dataset 5d. Number of persons with TD issued (flow)

This dataset refers to the number of persons for whom central, diplomatic or consular authorities of a given third country issued Travel Documents during a given reference month.
This category should also include persons identified during any of the previous reference months, for whom a Travel Document was issued during the current reference month.

Dataset 5e. Number of persons for whom negative replies to the identification request were received (flow)

This dataset should include the number of persons with regard to whom a verification/identification request/request for issuing a TD had been previously submitted to third country authorities, and during a given reference month a negative reply was received from the third country authorities.

Dataset 5f. ***Number of persons with pending replies to the identification request / no replies received (stock)***

This dataset should include the total (stock) number of persons with regard to whom a verification/identification request/request for issuing a TD had been previously submitted to third country authorities, but no reply has been received from the third country by the end the reference month, hence these cases are still considered as pending.

The dataset can include persons who have already been effectively returned before but, as a result of a rejected asylum application or having been found to be illegally staying, have been issued a return decision, thus starting the return procedure again.

Dataset 5g. Number of persons with identifications performed/Travel Documents issued within deadline (where applicable) (flow)

This dataset refers exclusively to citizens of third countries, with which EU readmission agreements are in force[7] or political arrangements specifying return procedures and deadlines have been concluded[8]. The agreements provide for specific deadlines for the process of readmission requests and subsequent issuing of travel documents for the purpose of return. The category should include the total number of readmission application processed and travel documents issued within the deadlines specified by the respective agreement.

---

7 For EU MS: Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Cape Verde, Georgia, FYROM, Hong Kong, Macao, Montenegro, Moldova, Pakistan, Russia, Serbia, Sri Lanka, Turkey, Ukraine. In the case of IRMA Countries not bound by EU readmission agreements, the relevant countries will be specified in an annex to this document based on information provided by the respective IRMA Countries.

8 Such as, e.g. the Joint Way Forward with Afghanistan for EU MS. In the case of IRMA Countries not bound by the above, the relevant countries will be specified in an annex to this document based on information provided by the respective IRMA Countries.

Dataset 6. Number of persons with EU Travel Documents readmitted by the third country (flow)

This dataset refers to the number of persons effectively readmitted by the third country based on a European Travel Document for return[9] issued either based on available proof of citizenship or following identification by the country of origin, regardless of whether a prior formal acceptance of readmission has been provided by the third country or not. In the case of IRMA Countries that do not use EU Travel Documents but their national equivalent, the number of persons returned with such a document will be reported.

This dataset gives information on the acceptance by third countries to readmit returnees on the basis of the EUTD. In the case of third countries with which readmission agreements have been signed, this is also a possible indicator on the level of implementation of the agreement.

Dataset 7. Number of persons whose readmission was refused at the border

This dataset refers to the number of persons whose readmission was refused at the border of the third country to which they were being returned despite the persons being in possession of valid travel documents proving their citizenship of the given country, travel documents issued by the consular authorities following verification of their citizenship, EU Travel Document for return if citizenship is well proven with supporting documents and readmission was agreed to by the third country.

This dataset, even if the numbers will be limited, give a strong signal of eventual lack of cooperation of a third country on readmission and return.

---

[9] This means until 8 April 2017 a European Travel document for return as established by the Council Recommendation of 30 November 1994 concerning the adoption of a standard travel document for the expulsion of third-country nationals (OJ C 274, 19.9.1996, p. 18); after 8 April 2017 also established by Regulation (EU) 2016/1953 of the European Parliament and of the Council of 26 October 2016 on the establishment of a European travel document for the return of illegally staying third-country nationals, and repealing the Council Recommendation of 30 November 1994, OJ L 311, 17.11.2016, p. 13–19

Dataset 8. Number of persons returned on charter flights

This dataset refers to the total number of persons issued a return decision effectively returned from the Member State during the reference month with the use of a charter flight. This includes both flights organised individually by the IRMA country, joint return operations and operations supported by the EBCGA.

Data Accuracy Assessment Sheet

The Data Collection will be accompanied by a Data Accuracy Assessment Sheet within the IRMA data collection web form to enable IRMA Countries providing national metadata information concerning the completeness and accuracy of the operational data provided.

This information should be updated in English, as necessary (at any given time) and as soon as the metadata concerning a given dataset changes (it is the responsibility of the IRMA Country to update this information in relation to the data sent). The consecutive versions of the evaluation sheet will be time-stamped and saved in the database, so that relevant comments concerning individual reference months can be automatically extracted together with data reporting.

The Data Accuracy Assessment Sheet will enable IRMA Countries to provide caveats and additional information i.a. on the completeness, accuracy and reliability of data. **Providing such caveats is obligatory for indicators where non-numerical values are provided.**

The reporting tool available in the IRMA EU Operational Data workspace will enable printing pre-formatted reports of the return Operational Data. Any such printouts will be automatically marked EU RESTRICTED at the bottom of the page. The report will also contain the caveats provided in the Data Accuracy Assessment Sheets.

Validation rules at the level of the Member State

Validation will be conducted between the data collection and the Data Accuracy Assessment Sheet. If the rule as set out in this table is not respected, an automatic error message will appear, warning the Data Submitter.

Rule	Error	Applicable to
if Total number of persons = 'N/Av', metadata = 'data not available' + justification provided	ERROR	All indicators
if Total number of persons = 'N/Ap', metadata = 'not applicable' + justification provided	ERROR	All indicators
if Total number of minors = 'N/Av', metadata = 'data not available' + justification provided	ERROR	1, 2a, 2b. 3. 4a, 4b.
if Total number of minors = 'N/Ap', metadata = 'not applicable' + justification provided	ERROR	1, 2a, 2b. 3. 4a, 4b.
Total number of unaccompanied minors = 'N/Av', metadata = 'data not available' + justification provided	ERROR	1, 2a, 2b. 3. 4a, 4b.
if Total number of unaccompanied minors = 'N/Ap', metadata = 'not applicable' + justification provided	ERROR	1, 2a, 2b. 3. 4a, 4b.

IRMA - Operational Data Collection User Charter

(Version 1.4 – 11 August 2017)

Introduction

Under the responsibility of your General Manager (GM), you have been entitled by your Operational Manager (OM) to be an actor in IRMA's Operational Data Collection (ODC) tool.

Further to the request received by your OM, DG HOME will grant you access to the ODC, as Operational Data collector or Operational Data submitter. Before doing so, DG HOME will make sure that you have approved this Charter.

Please read carefully the information below in order to be aware of what this Charter implies for you and for the use of the ODC tool. By approving this User Charter, you declare that you have read it and that you will comply with the requirements laid down in it once your access to the ODC tool has been granted.

By subscribing to this "Operational Data Collection User charter" I accept that:

- ✓ The password that will be used for accessing IRMA is owned by me and will not be given or transmitted, even temporarily, to a third party.
- ✓ I am aware that the data in the ODC are restricted and protected working data. I will abstain from any reproduction or public dissemination, in whatever form, of the content and the reports obtained via the ODC tool. If wishing to do so, I must request prior written authorisation from my GM for national data and from DG HOME for non-national data. DG HOME will ask the prior approval of MS involved before authorising any use of the data in question. I will continue to be bound by this clause after expiry of my access to the ODC tool.
- ✓ I understand that I am responsible for the security of the workstation I am using to access IRMA and the ODC tool and I must take the necessary measures to avoid interception of the information accessible through it (e.g. anti-spyware, anti-virus, auto lock feature, etc.).
- ✓ I am aware that the Commission may keep a log of all access to IRMA and its ODC tool for security purposes and for operational management.
- ✓ If I have a reasonable suspicion that a third person accessed the IRMA ODC tool through my IRMA user account, I will immediately inform my GM, OM and DG HOME's IRMA Team.
- ✓ If I do not respect this charter, I understand that the Commission will revoke my access immediately and without prior notice. In such a case, a justification will be sent to me, with copy to the OM and GM where further administrative and disciplinary measures may be undertaken by the concerned Member State.
- ✓ The Commission, in agreement with Member States, may review this Operational Data Collection User charter as deemed necessary.
- ✓ I have read and will respect the:
  - IRMA User Manual,
  - Operational Data Collection user manual,
  - Technical guidelines for return Operational Data Collection.
- ✓ In cases of doubt, I will seek the necessary advice and information regarding the collecting and accessing the operational data by contacting my OM, GM or, where appropriate, DG HOME's IRMA Team.

Name: Date: Signature:

European Commission, DG HOME C1, LX46, 1049 Brussels, BELGIUM - Tel. +32 22991111 – HOME-EC-IRMA@ec.europa.eu

Irregular Migration Management Application (IRMA) – Encryption of Exchanged Files

Abbreviations

1. IT: Information Technology
2. PGP: Pretty Good Privacy
3. PKC: Public-Key Cryptography
4. PKI: Public Key Infrastructure
5. RCA: Root Certification Authority
6. WoT: Web of Trust

Introduction

Public-Key Cryptography (PKC)

Nowadays, Public-Key Cryptography (PKC) or Asymmetric Cryptography is considered as the primary cryptographic scheme for securing the communication over the Internet, by providing the reliable identification of the communicating peers (e.g. users, workstations) and safeguarding the privacy of the exchanged information. The basic notion behind PKC is that each communicating peer possesses a unique Public cryptographic key and an equally unique Private cryptographic key. These Public and Private keys are always produced as a pair and they are both uniquely linked to (they uniquely identify) the respective communicating peer. Moreover, the Public/Private keys inherently hold the special attribute that **any data (e.g. files, messages) that are encrypted with a Public key can only be decrypted by using its pairing Private key**.

In this respect, according to the PKC scheme, each user in a networked community that needs to communicate in a secure and private manner is assigned with a pair of Public/Private keys. The Private key of each user is kept utterly secret, i.e. it is known only to the specific user. On the contrary, all the Public keys are made available to all the users of the concerned community by any possible means (e.g. by posting them in a commonly accessible repository). Thereafter, if user A wishes to encrypt data for user B, user A i) searches the Public key of user B in the commonly accessible repository of Public keys, ii) encrypts data of interest using the Public key of user B, and iii) finally sends these encrypted data to user B. As soon as user B receives the encrypted data, user B decrypts them using his/her own Private key.

Nevertheless, despite its high efficiency and its very broad applicability and deployment, PKC is still exposed to two basic attack vectors:

1. The secrecy (security and privacy) of the Private key of each user. Anyone that possesses a Private key can decrypt any data that have been encrypted with the pairing Public key.

    a. The most prominent solution to this issue is to have the pair of Public/Private keys produced at the user side and not by a third-party entity. This way, the Private key does not ever leave the possession of its user.

2. The authenticity of the Public key, i.e. the issue of whether the actual owner of a Public key is the physical person that is alleged to be. If a Public key is disseminated by a malicious actor under the fake identity of a legitimate user (e.g. if the Public key of a user is replaced by the Public key of a malicious actor keeping however the identity of the legitimate owner), then, by using this fake Public key, the forger will be able to decrypt any information that is being encrypted for the alleged owner (legitimate user) of the Public key.

    a. For tackling this issue a Public key Infrastructure (PKI) needs to be introduced and technically realised. The PKI is a detailed scheme for binding the Public keys to the physical identities of the actual users (or legal identities if the users represent an organisation as a whole) in an unconditionally trustworthy manner.

As a result, the two aforementioned attack vectors define respectively the two major security requirements that a PKC implementation needs to satisfy, in order its security to be safeguarded.

Pretty Good Privacy (PGP)

Within the broader PKC framework, Pretty Good Privacy (PGP) has been proposed as a specific implementation that focuses in particular on the architecture of the applied PKI scheme. In more detail, according to a common PKC approach, the owners of the Public keys are identified by means of digital certificates that are issued and managed by a central third-party entity. This third-party entity, which is usually referred to as Root Certification Authority (RCA), is by default accepted and trusted by all the members of the communicating community and it is responsible for validating the identity of the users and guaranteeing on this solid basis the authenticity of the shared Public keys. The overall procedure for the issuing and management of the certificates by the RSA along with the assignment and dissemination of the pairs of Public/Private keys follows sophisticated rules and workflows that are strictly predefined.

Nevertheless, although it provides an efficient solution for the second security requirement of the PKC (0.2), the centralised PKI architecture on the basis of an RCA presents the important drawback that its deployment and maintenance is rather complex and it requires extensive resources concerning both IT and logistics aspects. Hence, the centralised PKI architecture limits the application of the PKC only in cases of communicating communities where an RCA can be made available in a cost-efficient and time-efficient manner.

On the contrary, PGP supports a distributed architecture for the certification of the users' Public key (i.e. the verification that a Public key actually belongs to its declared owner). To this end, PGP is based on the Web of Trust (WoT). The rationale behind the WoT is that each Public key can be certified (signed) by any members of the community who rate it with different grades of trust. This way no RCA, holding the absolute knowledge and responsibility for certifying the Public keys, is necessary and every user that wishes to encrypt data for a given Public key can assess its authenticity based on his/her trust on the various members that have signed this Public key.

Despite its inherently distributed orientation, PGP does not exclude the deployment of an RCA or of any other means for authenticating and sharing the users' Public keys and which can be used either in combination or completely independently from the existing modules that are already built-in in PGP for supporting such functionalities. **This flexibility in the implementation of the PKI (i.e. of the means for authenticating and managing the Public keys) is the major advantage of PGP that is leveraged for the purposes of IRMA. Being more specific, IRMA fully controls the identity of its users. Consequently, deploying an PKI on the basis of IRMA (i.e. the Public keys will be disseminated through IRMA) safeguards the authenticity of the Public keys and therefore it is not necessary to resort to a third-party RCA for additional certification.**

IRMA PGP-based Public Key Cryptography Scheme

As far as data encryption is concerned, IRMA should be able to support the encryption of the files that are exchanged among its users whenever this is deemed necessary by the users themselves. Being more specific, the common use case scenario that needs to be supported is the following:

An IRMA user A should be able to encrypt a file and share it with any other IRMA users by putting it as an attachment to a content item of any of the IRMA features that accommodate file sharing (e.g. Messages, Articles, Events, Requests). Regardless of who may be able to access the file after its encryption, either inside IRMA (i.e. the IRMA users that have access permissions for this specific content item that the encrypted file is attached to) or outside IRMA (i.e. any person that may have access to a workstation or data storage medium where the encrypted file has been downloaded from IRMA), this encrypted file should only be possible to be decrypted by the IRMA users that have been specifically defined by the IRMA user A at the moment that the initial file was being encrypted. Hence, the encryption of the exchanged files of interest should not only cover the files' presence inside IRMA, but these files should be encrypted in an end-to-end manner.

In accordance with this common use case scenario and taking into account the characteristics, requirements and capabilities of the IRMA platform and of the respective community of users, **PGP has been selected as the most adequate solution for providing file encryption in IRMA**. At this point, it must be underlined that

1. **The IRMA PGP-based PKC Scheme regards solely the encryption of files that are exchanged as attachments to any IRMA content item and it does not concern any other data or pieces of information in general that may be inserted to IRMA**.

2. **The IRMA PGP-based PKC Scheme offers the end-to-end encryption of the exchanged files. This means that the file to be exchanged is encrypted at the sender's workstation before it is uploaded to IRMA and it is downloaded still encrypted at the receiver's side.**

3. **IRMA provides to its users the means for encrypting files that will only be possible to be decrypted by specific other IRMA users. This is an action that is not applied automatically to all the exchanged files, but the IRMA users carry out the encryption (decryption) at their own workstations before (after) the uploading (downloading) of the files to (from) IRMA.**

4. **The unique additional IT requirement for the IRMA PGP-based PKC Scheme to be supported at the users' side is the installation of a PGP-compliant software at the IRMA users' workstations**. Such a PGP-compliant software could be Gpg4win [1]. The exact details for the production of the Public/Private keys as well as for the file encryption/decryption using Gpg4win is described in the Annex.

5. **Thanks to its end-to-end rationale, the IRMA PGP-based PKC Scheme completely decouples the encryption/decryption of the files from their exchange through IRMA. The exchanged files do not have to be encrypted/decrypted at the workstation that IRMA is accessed from but the encryption/decryption can be potentially executed in another workstation where the aforementioned PGP-compliant software is installed.**

6. **The IRMA PGP-based PKC Scheme concerns only the IRMA user that wish to participate either as senders (encrypt a file) or as receivers (decrypt a file) in the exchange of encrypted files. The rest of the IRMA users can continue using IRMA perfectly normally without considering the IRMA PGP-based PKC Scheme**.

The possible schemes for the production and management of the Public/Private keys as well as for the exchange of encrypted files by means of the IRMA PGP-based PKC Scheme are presented hereafter.

Production and Management of the Public/Private Keys in IRMA

According to the IRMA PGP-based PKC Scheme, the Public keys of all the users will be disseminated by means of IRMA.

1. The IRMA user profile supports the storage of the user's Public key in a dedicated field.

2. The Public key of each IRMA user will be possible to be viewed and downloaded by any other IRMA user, by accessing the user profiles in the repository of IRMA users. In the repository of IRMA users, any IRMA User can

    a. View the list of all the IRMA users, grouped by Primary Organisation and Organisational Entity.

    b. Search for other IRMA users based on their name, Primary Organisation and/or Organisational Entity, Additional Memberships and Role in Return Activities for each one of their Organisational Entities and Additional Memberships.

Moreover, each user's Private key needs to be stored at the same workstation where the file encryption/decryption will be executed.

Finally, in order the file encryption/decryption to be executed, a PGP-compliant software is necessary to be installed at each user's workstation where the file encryption/decryption will be executed.

By utilising IRMA for disseminating the users' Public keys, the IRMA PGP-based PKC Scheme adopts a centralised PKI architecture where IRMA practically plays the role of the RCA. This way the advantages of PGP are efficiently combined with the reliability of the centralised PKI architecture, which guarantees the authenticity of the Public keys and the individual users do not need to assess themselves the identity of their peers.

As a matter of fact, IRMA can be considered as a perfectly efficient solution for these purposes, since the physical identity of the IRMA users is thoroughly examined both during their initial application and periodically, while IRMA offers a secure environment for sharing the Public keys. Hence, it is not necessary to resort to the issuance of certificates from a third-party RCA for guaranteeing the authenticity of the Public keys, but IRMA can provide this functionality in an utterly reliable manner.

In this respect, there are two schemes that can be considered for the production and management of the Public/Private keys, taking into account the scope of the IRMA community and exploiting the IRMA infrastructure. The first scheme is **user-initiated** and the second one is **IRMA-initiated**. They differ with each other in the level of user involvement that they require as well as in their efficiency with respect to the two PKC security requirements (0.1 and 0.2).

i. User-initiated Public/Private Key Production and Management

According to the user-initiated scheme for the production and management of the Public/Private keys in IRMA:

1. Each IRMA user should produce his/her own pair of Public/Private keys.
    a. In order the files to be possible to be encrypted/decrypted to be carried out, a PGP-compliant encryption/decryption software is necessary to be installed at the users' workstation. This exact same software will also be used for producing the user's Public/Private keys (Annex).
2. The Private key is automatically stored at the user's workstation where it was produced.
3. Each IRMA user should export the Public key from the PGP-compliant software where the pair of Public/Private keys was produced.
4. Each IRMA user should update his/her user profile in IRMA by uploading in it the Public key that was previously exported.

By having the pair of Public/Private keys produced by the users themselves (or at least at the users' workstation), the secrecy of the Private key is unconditionally guaranteed, since the Private key is continuously under the possession of its owner and it is not shared with any other IRMA user or person in general. Hence, the user-initiated scheme satisfies completely the first security requirement of the PKC (0.1).

It must be stressed out that the procedure for producing the pair of Public/Private keys does not necessarily have to be carried out by the users themselves, but it can be executed within the framework of the users' Organisational Entity (e.g. by the IT department). The security is not compromised at all as long as the Private key is produced at the users' workstation where the files will be encrypted/decrypted and it is not copied out of it. Similarly, the overall procedure of producing the pair of the Public/Private keys can be carried out centrally per Organisational Entity by the respective IT department/personnel and installed to the users' workstation, so as to minimise the involvement of the users in the IT details.

Moreover, by disseminating the Public keys through IRMA as part of the IRMA user profiles, the authentication of the Public keys (i.e. identification of the physical person that actually owns the Public key) is adequately safeguarded, since:

1. The physical identity of each IRMA user is scrutinised during the validation of his/her IRMA New Access Application for the provision of the new IRMA as well as during the periodical revalidation of all the users. This initial validation and periodical revalidation is carried out at three levels: a) by the user's corporate e-mail address, b) by the Operational Managers of the user's Organisational Entity, and c) by the IRMA Super Users. Therefore, the identification of the physical person behind the IRMA account efficiently performed.

2. The users' access to IRMA is realised through a secure Internet connection (i.e. https). Therefore, the Public key cannot be modified during its upload from the user to IRMA.

3. IRMA is hosted in a secure environment and the users' authentication to IRMA (i.e. login) is carried out using the secure EU Login infrastructure. Therefore, a user profile in IRMA can only be edited by the respective authenticated user.

Consequently, the user-initiated scheme satisfies sufficiently the second security requirement of the PKC (0.2).

ii. IRMA-initiated Public/Private Key Production and Management

According to the IRMA-initiated scheme for the production and management of the Public/Private keys in IRMA:

1. The pair of Public/Private keys for each IRMA user is produced centrally in IRMA by the IRMA Administrators.
    a. Each Private key is sent to the respective IRMA user by means of IRMA (e.g. IRMA Message).
2. Each IRMA user should import the received Private key to the PGP-compliant software that is installed at the workstation where the file encryption/decryption will be carried out.
3. The Public key of each IRMA user is uploaded by the IRMA Administrators in his/her user profile.
    a. The IRMA Administrators should be provided with the access permissions to edit the Public key in the user profile of the IRMA users.

By having the pair of Public/Private keys produced centrally at IRMA, the security could be in theory compromised, since the activity of the IRMA Administrators introduces by default a security breach due to this intervention of human factor that is external to the cryptography workflow. In more detail,

1. The Private key is produced outside the users' workstation and it is thereafter sent to users so as to be imported to the PGP-compliant software at their workstation. **Hence, the first security requirement of the PKC is not adequately covered by the IRMA-initiated scheme (0.1).** In addition, the import of the sent Private key requires exactly the same level of user involvement that would be required for its production according to the user-initiated scheme. **Thus, there is no benefit in terms of complexity and user experience and convenience with respect to the user-initiated scheme.**

2. The Public key is uploaded to the IRMA user profiles by the IRMA Administrators, i.e. the shared Public key is not controlled by the users themselves. **Consequently, the second security requirement of the PKC is not adequately covered by the IRMA-initiated scheme (0.2).** The only possible advantage in comparison with the user-initiated scheme is that the IRMA users do not have to upload their Public key to their user profile on their own. **However, not even this is a valid advantage, since uploading the Public key to the user profile is a very simple, quick and well standardised procedure, which should require almost the same amount of time that will be necessary in the case of the IRMA-initiated scheme for the users to send their Public keys to the IRMA Administrators by an IRMA Message.**

Additional Security Measures

In order to further safeguard the security of the IRMA PGP-based PKC Scheme, some additional security measures, particularly tailored to the requirements and functionalities of the IRMA PGP-based PKC Scheme, will be introduced to the existing IRMA infrastructure:

1. IRMA will provide a user-friendly tool, so that the IRMA users will be able to easily report any possible forging of their Public key as this is stored in their user profile in IRMA.

    a. The concerned IRMA user will report the issue to IRMA by a single click of a button and his/her Public key will be automatically removed from his/her user profile in IRMA. Hence, no IRMA user will be able to encrypt files with the forged Public key and there will be no danger of exposing these files to unauthorised access.

2. Whenever a modification is made to the Public key of an IRMA user (i.e. the Public key that is stored in IRMA as part of the user profile), an e-mail notification will be sent to this IRMA user.

    a. Since the success of an IT attack cannot be completely excluded, the use of notifications is nowadays considered as one of the most efficient response measures against malicious IT activity. For example, it is a common approach to send notifications about electronic financial transactions, access to corporate/personal intranet/Internet accounts etc.

    b. The sending of notifications, combined also with the aforementioned reporting tool, is expected to render totally ineffective any malicious modifications in the stored Public keys.

    c. The sending of notifications by means of SMS could also be considered.

3. IRMA will provide a user-friendly tool, so that the IRMA users will be able to easily compare the version of their Public key that is stored in their workstations with the version of their Public key that is stored in their user profile in IRMA.

    a. If the comparison fails, the concerned Public key will be automatically removed from from their user profile in IRMA.

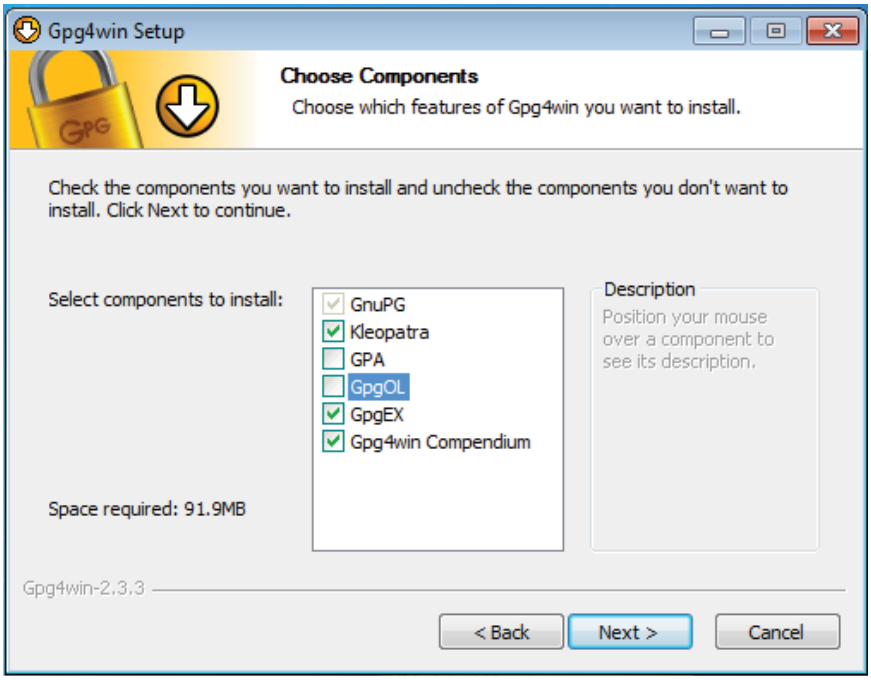
    b. This comparison will be mandatory during the periodical revalidation of the IRMA User Accounts.

4. The EU Login scheme, which is used for the authentication of the users in IRMA, supports a 3-point authentication, i.e. apart from their username and password the users can be requested to provide a third additional piece of information (e.g. a one-time-password that is sent to the users by SMS).

Annex A. Installation of Gpg4win

1. The Gpg4win software should be installed at the workstation where the file encryption/decryption will be executed.
2. Visit the Gpg4win website (https://www.gpg4win.org/) and download the executable file.

3. Run the executable file that you downloaded in Step-AnnexA-2.
4. Unselect the option GpgOL

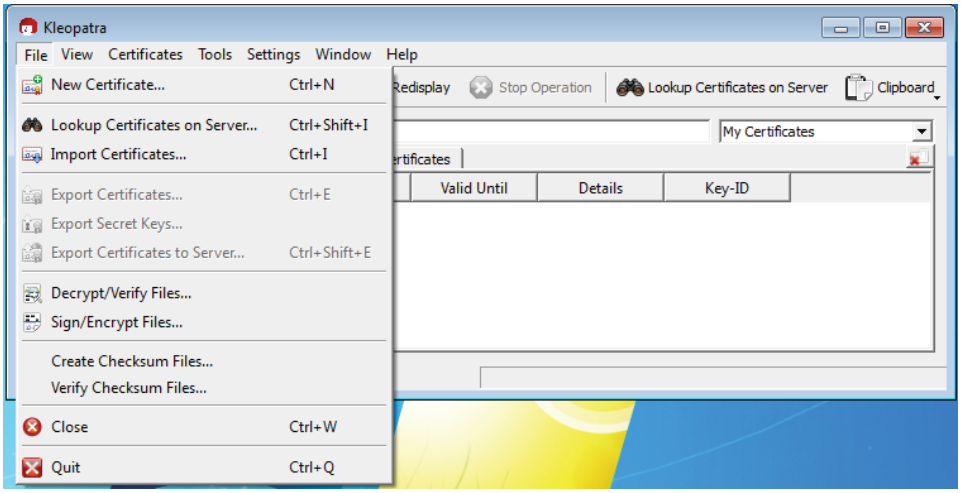


5. Click on Next in the consecutive windows until the installation is completed.
6. A software named Kleopatra has been installed at your workstation among others. This is the software that will be used for the management of the pair of Private/Public keys and for the encryption/decryption of files.

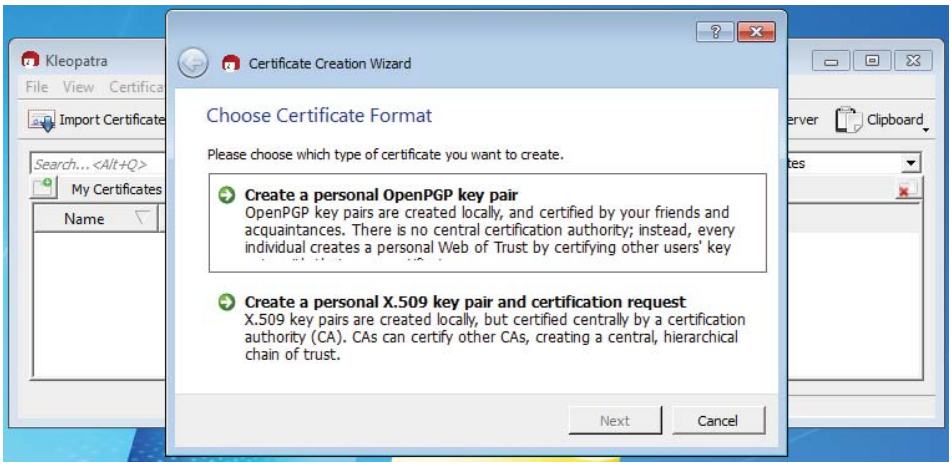
Annex B. Public/Private Keys Management with Gpg4win

I. Creation of the Pair of Public/Private Keys

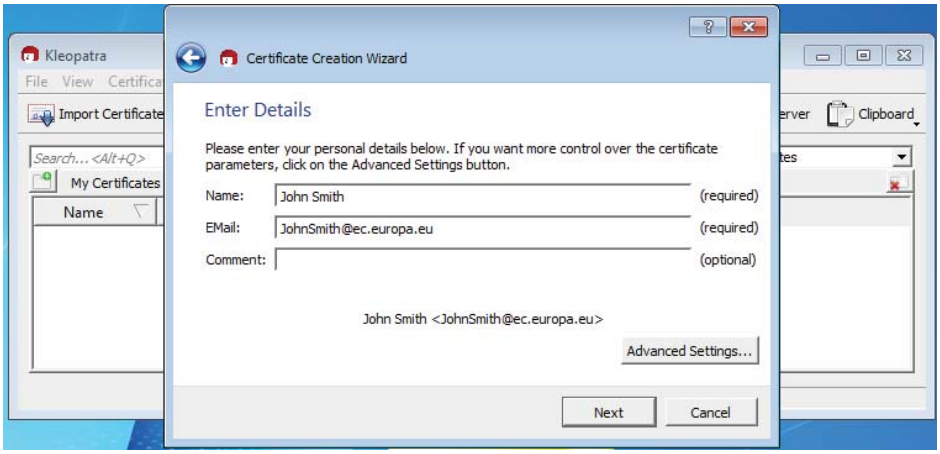
1. Open the Kleopatra software.
2. Click on File -> New Certificate.



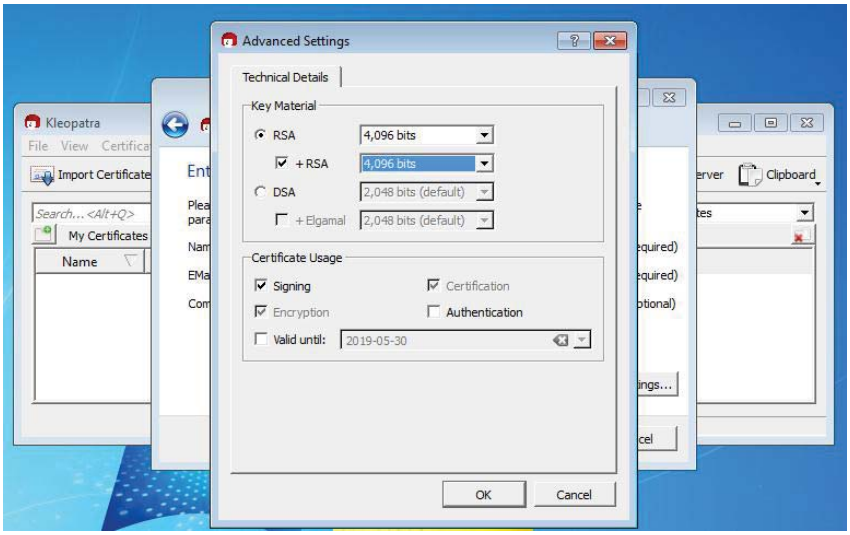
3. Select Create a personal OpenPGP key pair.



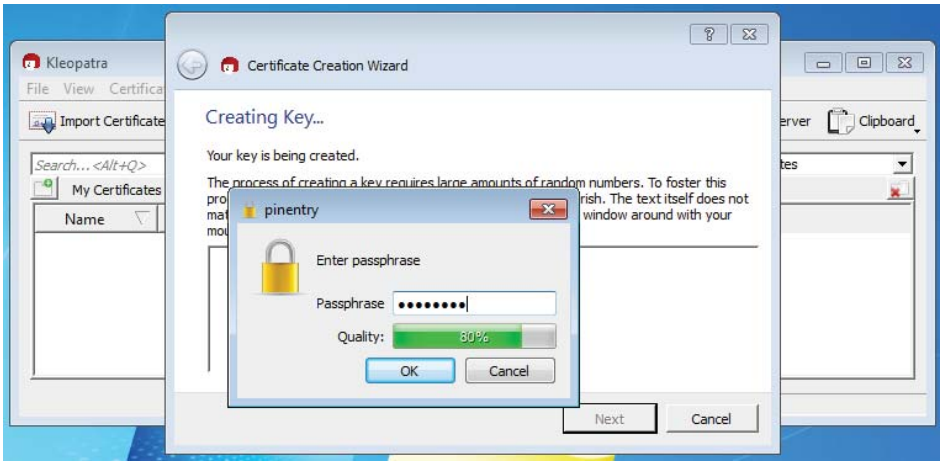
4. Complete your name and your e-mail address.
    a. Your name should be completed with standard Latin characters.
    b. The provided name and e-mail address should be the same ones that you are using in IRMA.



5. Do not click on Next, but click on Advanced Settings
    a. Select
        - RSA: 4,096 bits
        - +RSA: 4,096 bits
    b. The rest of the options should be left with the default configuration.
    c. Click on OK.

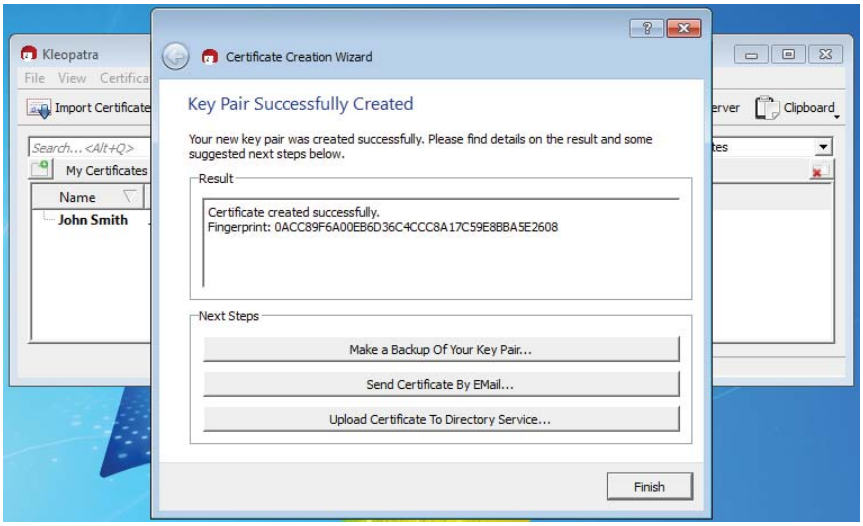


6. Click on Create Key
7. Provide a passphrase (i.e. password).
    a. You will be requested to provide this passphrase every time you wish to decrypt a file.
    b. Someone getting hold of your Private key must also have this passphrase to use it.
    c. Do not share this passphrase with anyone.



8. Retype your passphrase for confirmation.
    a. Click on OK.

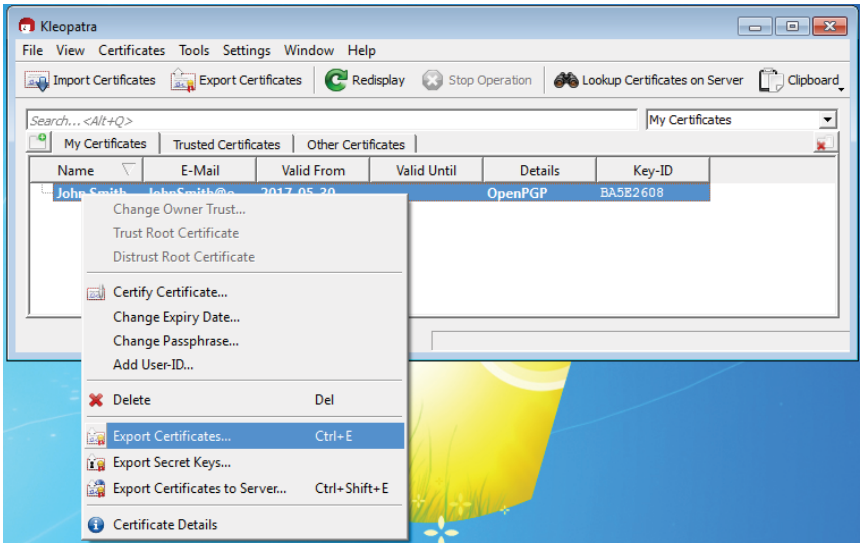
9. You see the message Key Pair Successfully Created. This means that your pair of Public/Private keys has been successfully created and installed at your workstation.
    a. Click on Finish.



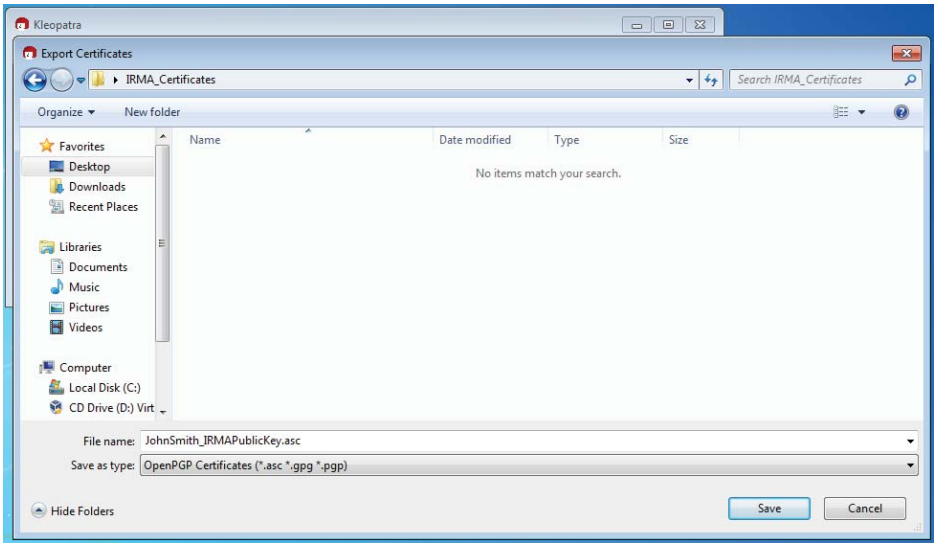
10. Your Private key has been automatically stored in the Kleopatra software at your workstation.

II. Export of the IRMA User's Own Public Key

1. You need to export your Public key and save it as a separate file, in order this file to be shared with the rest of the IRMA community, by uploading it to your user profile in IRMA.
2. Open the Kleopatra software.
3. Find your own Certificate (pair of Public/Private keys) under the tab My Certificates and right click on it.

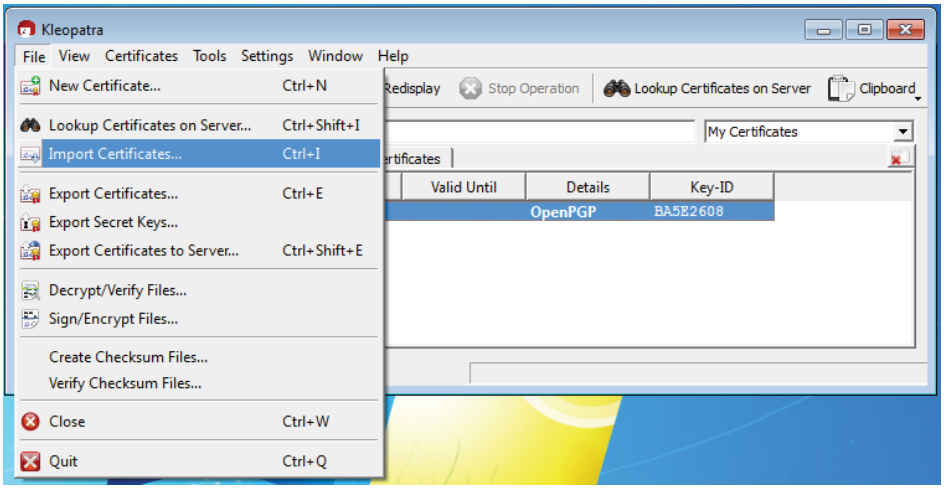


4. Click on Export Certificates.
5. Save your Public key as a file locally at your workstation.
    a. Provide a self-explanatory name for the file

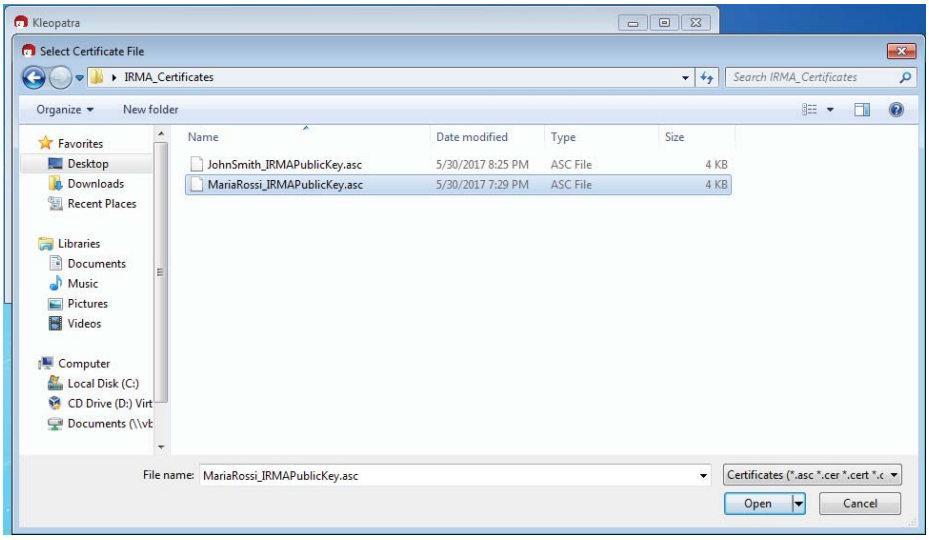


III. Import of the Public Key of Other IRMA Users

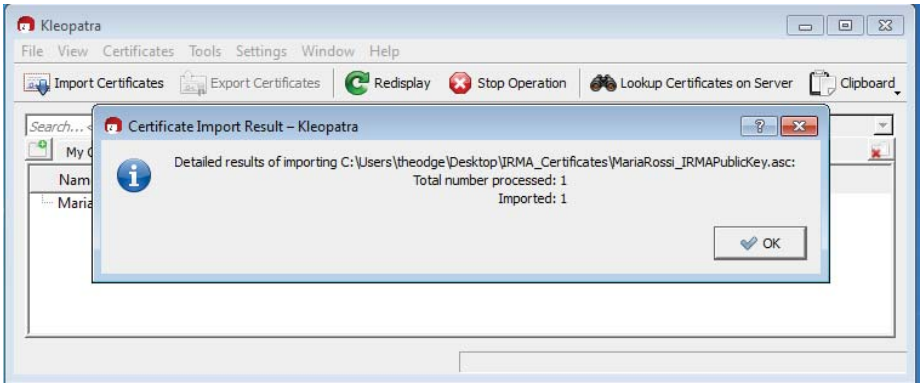
1. In order to encrypt a file that will be possible to be decrypted by another IRMA user, you first need to import the Public key of this IRMA user to your workstation.
2. Download from IRMA the Public key of the IRMA user that you wish to encrypt the file for.
    a. Save it locally at your workstation.
3. Open the Kleopatra software.
4. Click on File -> Import Certificates



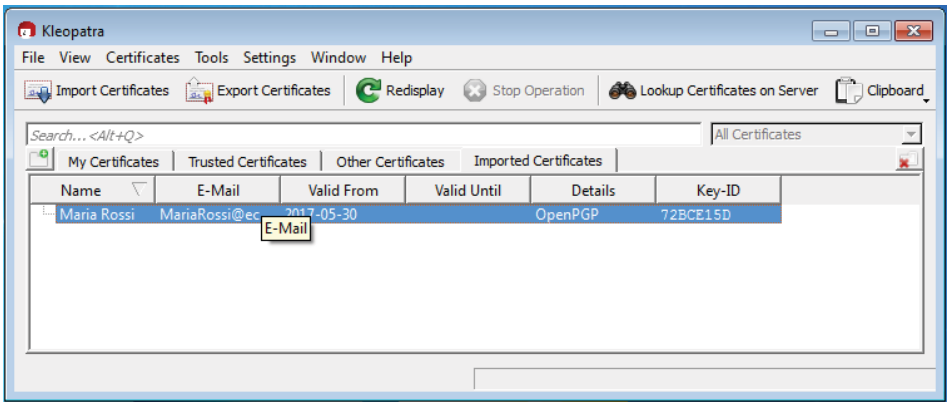
5. Browse your workstation and select the Public key of the IRMA user that you wish to encrypt the file for, i.e. the file that you downloaded at Step-AnnexB-III-2.



a. Click on Open.

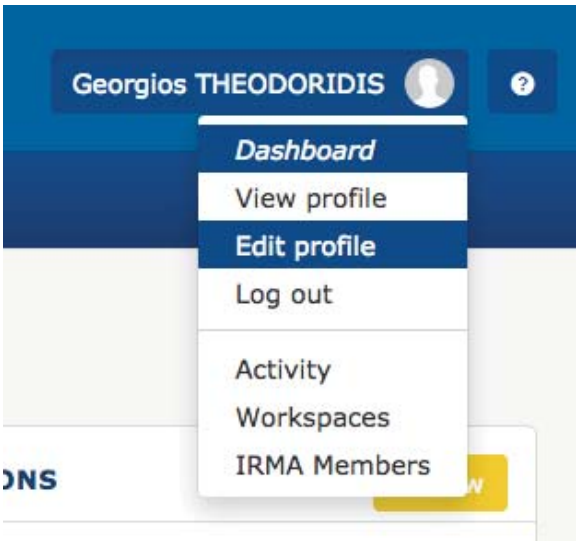


6. You will find the imported Public keys of the other IRMA users under the tab Imported Certificates.

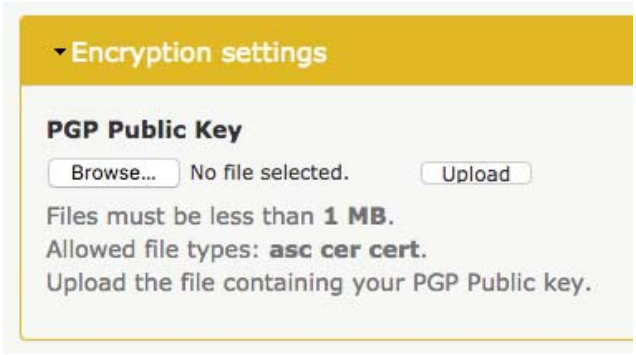


Sharing of the IRMA User's Own Public Key

1. According to the IRMA PGP-based PKC Scheme, the Public keys are shared by means of IRMA.
2. You need to upload your Public key in your user profile in IRMA, in order your Public key to be made available to the rest of the IRMA users and allow them to encrypt files that will be possible to be decrypted by you.
3. Go to IRMA -> Dashboard -> Edit Profile.



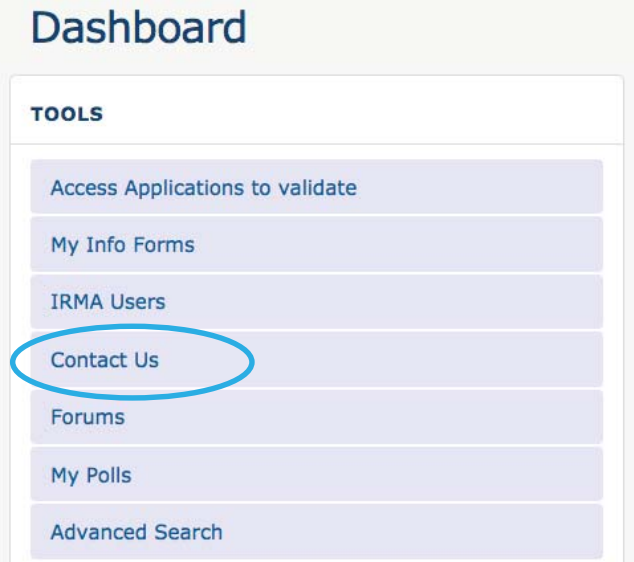
4. Go to Encryption Settings, in the tab Account (it is the default view when you access the Edit Profile feature).



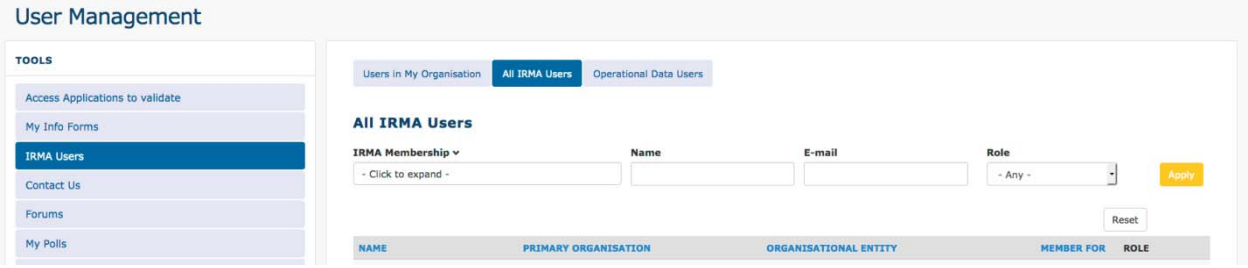
5. Browse your workstation and select your Public key, i.e. the file that you saved at Step-AnnexB-II-5.
6. Click on Upload.

IV. Obtaining the Public Key of Other IRMA Users

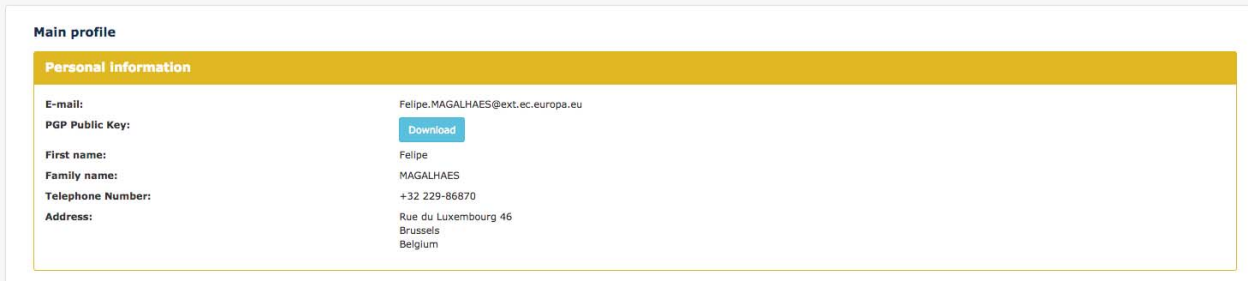
1. In order to find and obtain the Public key of other IRMA users, you have to view their user profile in IRMA.
2. Go to IRMA -> Dashboard -> IRMA Users.



3. Click on the tab All IRMA Users.
4. Search the IRMA users that you are looking for on the basis of any of their attributes.



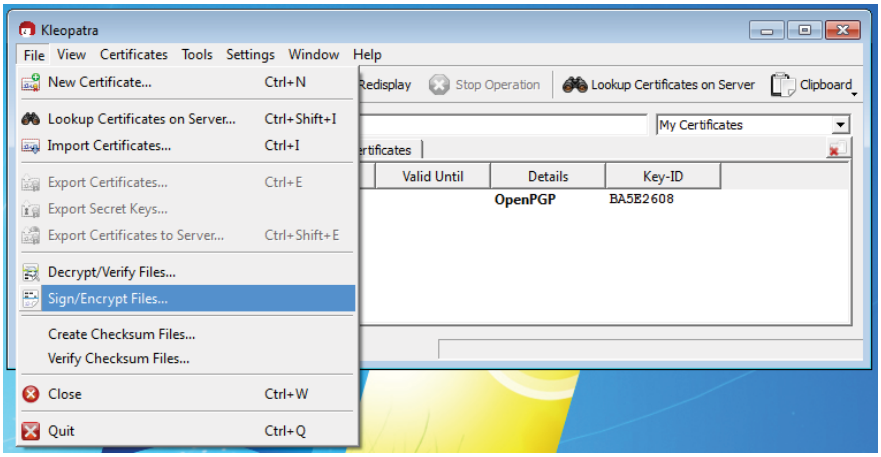
5. Click on the IRMA User of interest



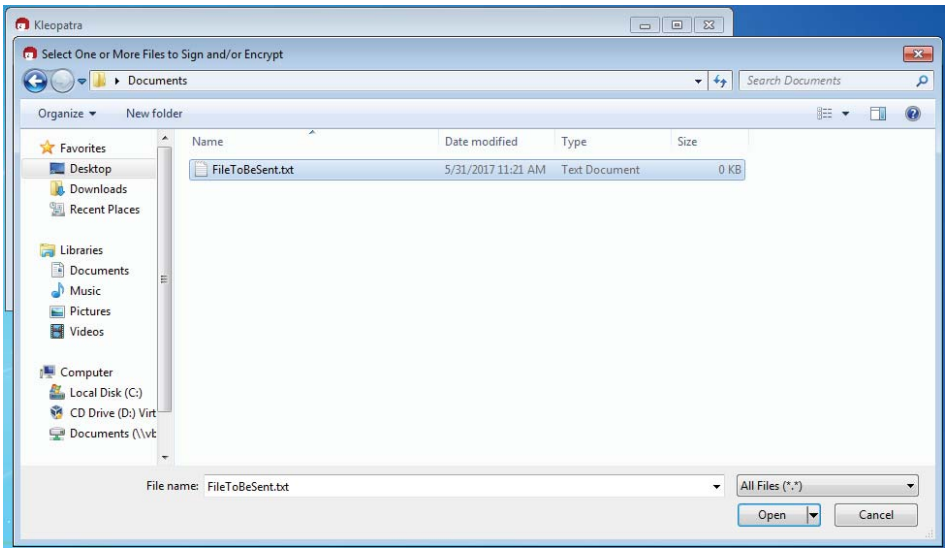
Annex C. Files Encryption/Decryption with Gpg4win

I. Encryption of the Exchanged Files

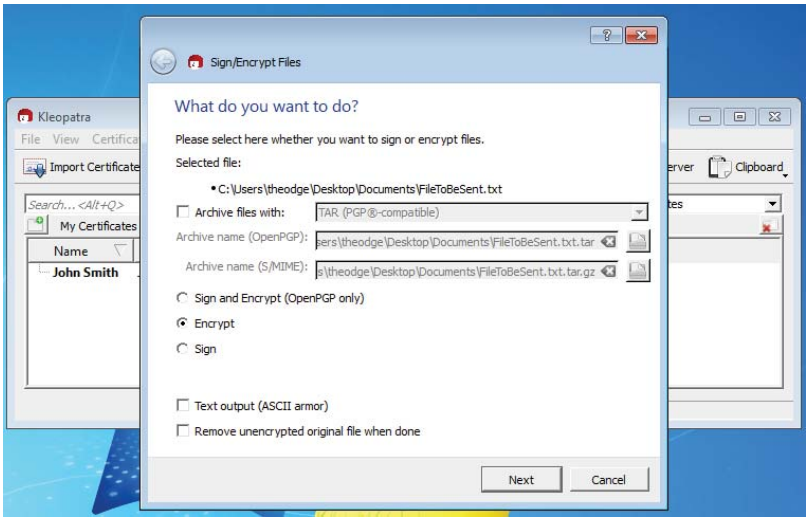
1. Open the Kleopatra software.
2. Click on File -> Sign/Encrypt Files.



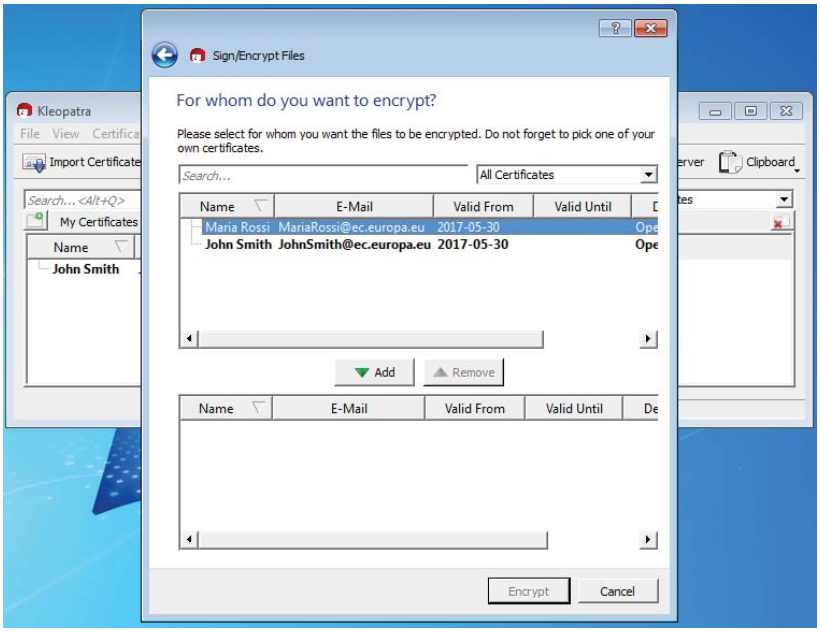
3. Browse your workstation and select the file that you wish to encrypt.
    a. Any file type can be selected without any limitation whatsoever.



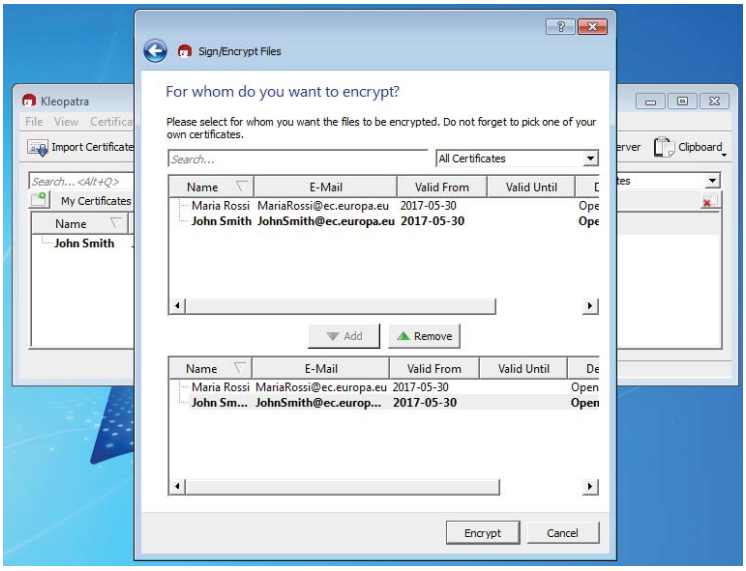
4. Leave the default configuration



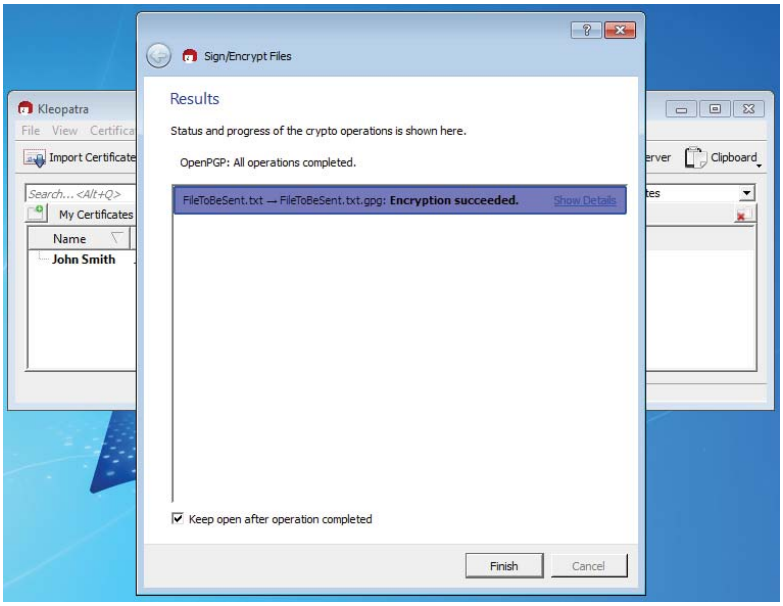
5. Select the IRMA users that you wish to be able to decrypt the file after it is encrypted.
    a. Select each concerned IRMA user and click on Add.



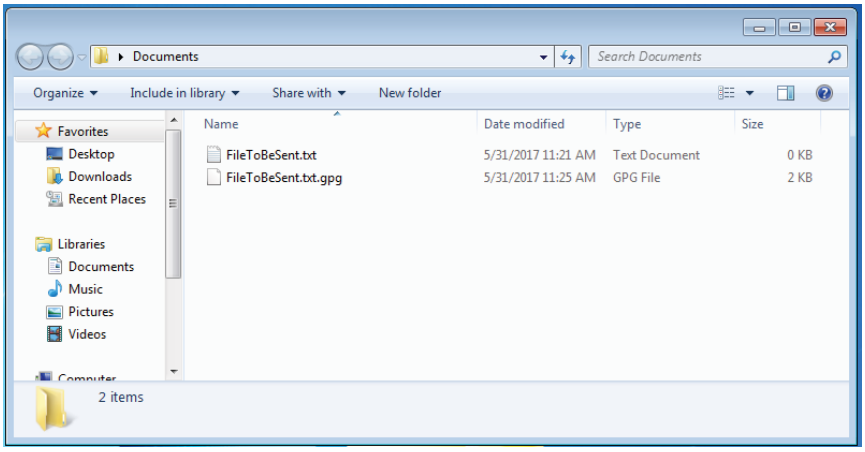
    b. Make sure that you also select yourself.
        - Otherwise you will not be able to decrypt the encrypted file, although you are the one that has encrypted it.
        - Decrypting the encrypted file may be proven useful for you, e.g. for checking/verifying the content/version of the file at a later stage.



6. Click on Encrypt.
7. The encryption of the file has been completed.



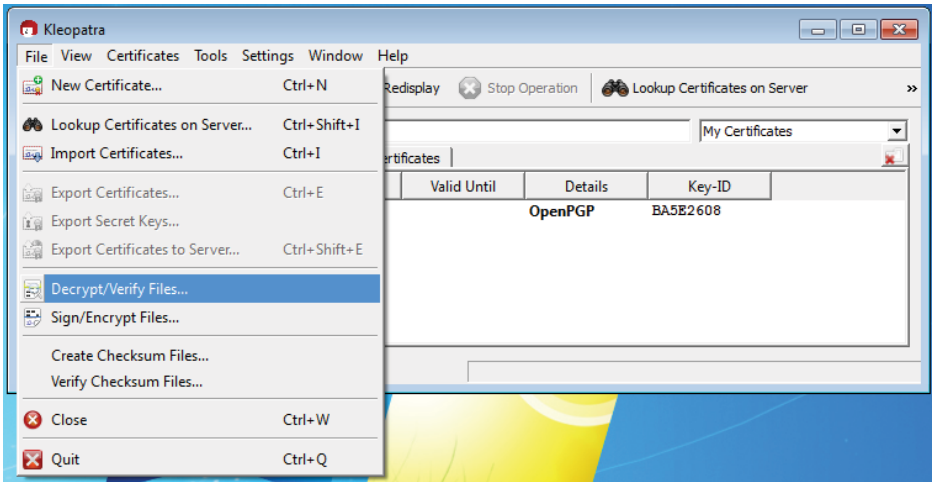
8. The encrypted file has been stored in the same folder where the initial prototype file lies.
    a. The name of the encrypted file is exactly the same with the name of the initial prototype file, plus the additional extension .gpg.



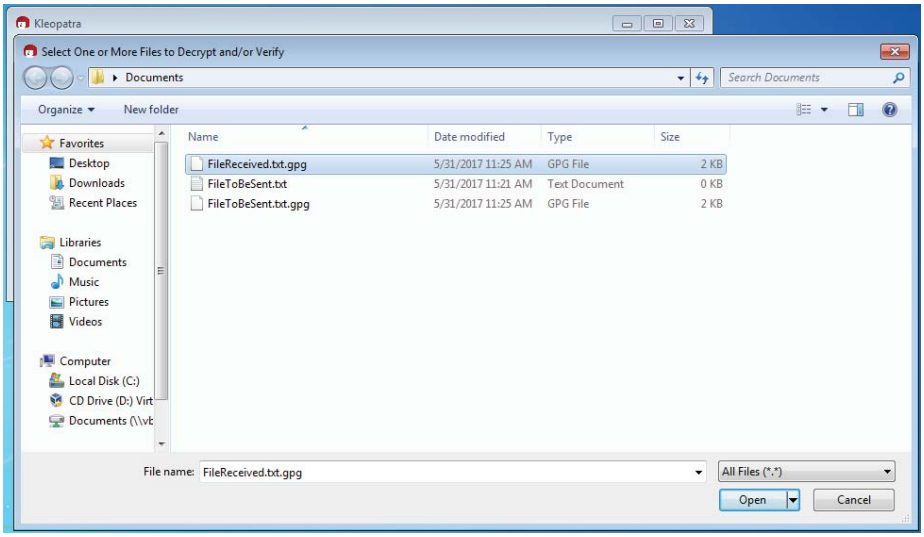
9. You may now share the encrypted file by putting it as an attachment to any suitable feature in IRMA.
    a. Regardless of who may have access to this encrypted file (through IRMA or when the file is downloaded at a workstation or if the file is stored in USB stick), only the IRMA users that this file is addressed to (i.e. the IRMA users that have been selected in Step-AnnexC-I-5) will ever be able to decrypt it.

II. Decryption of the Exchanged Files

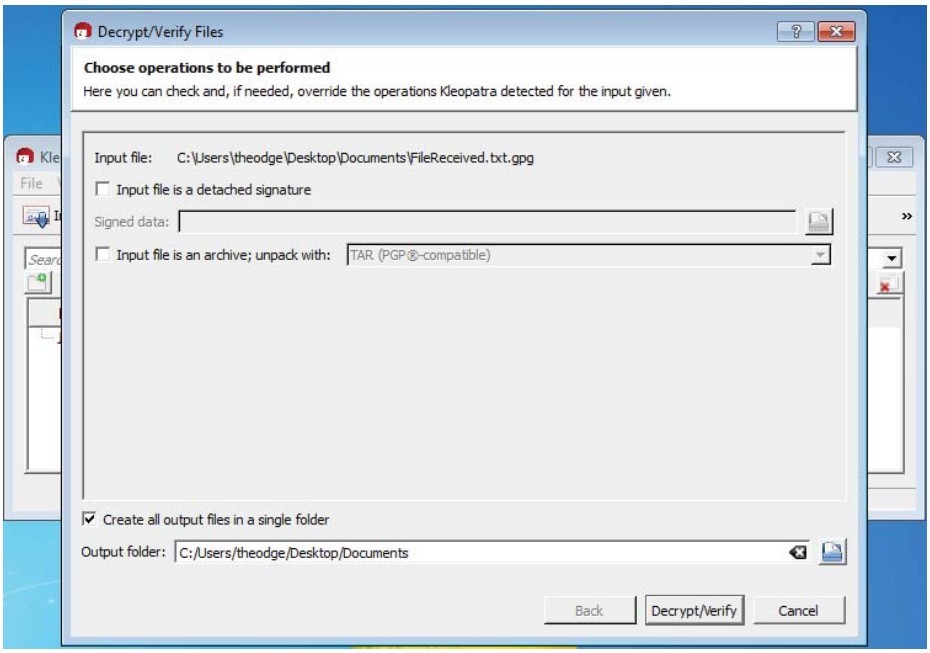
1. Open the Kleopatra software.
2. Click on File -> Decrypt/Verify Files.



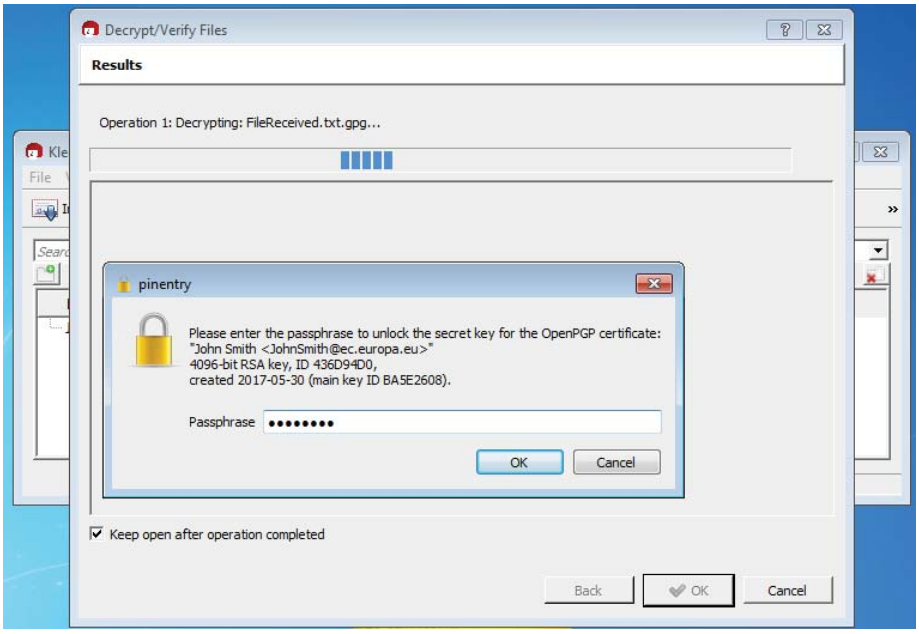
3. Browse your workstation and select the encrypted file that you have downloaded from IRMA.
    a. The file must have the extension .gpg



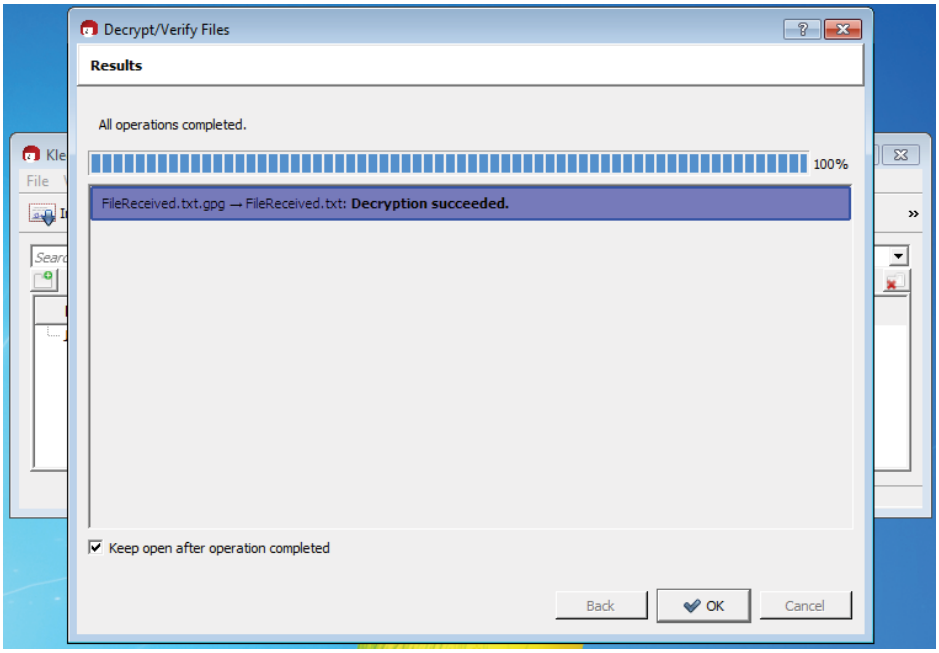
4. Leave the default configuration



5. Enter your encryption password, i.e. the passphrase that you provided when you created your pair of Public/Private keys (Step-AnnexB-I-7).



6. Click on Decrypt/Verify
7. The decryption of the file has been completed.



8. The decrypted file has been stored in the same folder where the initial encrypted file lies.
    a. The name of the decrypted file is exactly the same with the name of the initial encrypted file, without the additional extension .gpg.