Public Documents
Registration of authorities in IMI

Guide for Access managers

6th August 2018
Version 2

PUBLIC DOCUMENTS -REGISTRATION GUIDE

Document revisions

Date	Version number	Document changes
29/06/2018	0.1	First draft
11/07/2018	0.2	First revision
31/07/2018	1.0	Final revision for the launch
03/08/2018	1.1	Completed final version
06/08/2018	2	Content review

PUBLIC DOCUMENTS -REGISTRATION GUIDE

Table of Contents

1 Introduction 4

1.1 ....Scope and purpose 4

1.2 ....Legal Background 4

1.3 ....The IMI System 4

2 Access managers in IMI 5

2.1 ....Who can set up / register authorities and users in IMI? 5

2.2 ....How can NIMICs nominate new Access managers? 5

2.3 ....How to check if an authority has Access manager role? 6

3 Registering / setting up new authorities 7

3.1 ....Which authorities should be registered first? 7

3.2 ....Overview of the steps for setting up new IMI authorities 8

4 Registering users and user management 19

4.1 ....Registering additional users 19

4.2 ....Usernames, temporary passwords and first login to IMI 20

4.3 ....Editing and deleting registered users, resetting passwords 21

5 After the Registration 22

5.1 ....Updating the data of registered authorities 22

5.2 ....Suspending accesses and deactivating a registered authority 22

6 Further support 23

Annex I – Registration forms 24

1 Introduction

1.1 Scope and purpose

This document is drafted for National IMI Coordinators and IMI Access managers, who are responsible for the registration of authorities in the area of Public Documents.

It explains how to:

- **set up or register the coordinators and authorities** responsible for the Public Documents in the Internal Market Information (IMI) System
- **grant access** to the following modules within the IMI System:
  - Public Documents - Repositories (models of documents and samples of forged documents)
  - Public Documents - Request for information (concerning the authenticity of documents)

1.2 Legal Background

The **Regulation (EU) 2016/1191**, on promoting the free movement of citizens by simplifying the requirements for presenting certain public documents in the European Union, establishes that Member States must be able to check samples of the public documents to compare them to the copies they receive and assess their authenticity. In case of doubts, with regards to the authenticity of documents, authorities to whom a public document is presented should be able to send a request to verify the authenticity to the issuing Member State and its authorities.

To allow this, two modules are available in IMI:

- Public Documents - Repositories (models of documents and samples of forged documents)
- Public Documents - Request for information (concerning the authenticity of documents)

1.3 The IMI System

The Internal Market Information (IMI) System is a secure, multilingual online information exchange tool. It was developed to facilitate the exchange of information between public administrations across the EEA and the European Institutions and Bodies involved in the practical implementation of EU law.

For more information on terminology and use of the IMI System (login, search, translation and report generation features, support etc), please refer to the IMI User Handbook available on the IMI website:

http://ec.europa.eu/internal_market/imi-net/

2 Access managers in IMI

2.1 Who can set up / register authorities and users in IMI?

The tasks described in this document can only be carried out by IMI users who have '**Administrator**' right and whose authority is assigned the '**Access manager'** role in the IMI System.

By default **all authorities, which are National IMI Coordinators (NIMICs), have been assigned the 'Access manager' role**. In addition, several Member States have nominated special Access managers, who are responsible for registering and setting up authorities in a given legal area or for a given geographical territory.

> *In Romania, for example, the Ministry of Education was given the Access manager role to manage authorities and users in the area of professional qualifications. Countries with a strong regional and federal administrative structure, like Spain or Germany, nominated Access managers for each autonomous community/federal state.*

With regards to **registering/setting up IMI authorities in the area of Public Document**, National IMI Coordinators (NIMICs) may decide to take care of the administrative tasks themselves or to nominate another IMI authority as an Access manager and delegate the responsibilities for setting up authorities to this latter.

2.2 How can NIMICs nominate new Access managers?

If a NIMIC would like to nominate a new Access manager in IMI, first he/she needs to identify the authority in the system. If the "future" Access manager is not yet registered in IMI, the NIMIC needs to register it.

Once the future Access manager is identified in IMI, the NIMIC has to contact the IMI Helpdesk and ask the EC services to assign the Access manager role to the identified authority, with a short explanation of why the given authority should be an Access manager and which authorities it is expected to manage in future.

The IMI Helpdesk takes care of the technical assignment of the Access manager role as soon as possible (usually no more than a day); in case of questions the IMI Helpdesk contacts the NIMIC who nominated the Access manager.

*The **Access manager role** in IMI is a purely administrative role for authorities. It should only be assigned to those competent authorities who will support other authorities and users, will take care of administrative tasks like password resets and who will be responsible for registering and setting up other authorities in their area of competence.*

***On the contrary, authorities who will only supervise the information exchanges** of other authorities and will only need to monitor the use of IMI in the area of public documents **do not need to be assigned an Access manager role**, unless they are also taking care of the registration of authorities!*

***The Access manager role is assigned to authorities and not to IMI users**. Users who need to carry out tasks related to the management of other authorities and users a) must be registered for an authority that has the Access manager role and b) must be assigned an Administrator role. Users who belong to an IMI Access manager and are not responsible for authority and user administration in the system should not have administrator rights.*

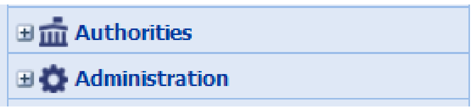
2.3 How to check if an authority has Access manager role?

The authorities that have the Access manager can be easily checked via the authority search in IMI, i.e. via the Authorities/Search or the Administration/Managed authorities menu option. Both searches include the Authority role criterion, where Access manager can be selected as a role.

Note that the latter menu option is only available to those users of the IMI Access managers, who have administrator rights.

You can easily verify if you have the right to manage other IMI authorities and users (I.e. if your authority has the Access manager role and if you have Administrator rights):

1. If your menu includes the **Administration** option that means that you have Administrator rights.



2. If under the **Administration** menu option you can find the **Managed authorities** and the **Register new authority** sub-items, that means that your authority is an Access manager and you can manage other authorities and users.

3 Registering / setting up new authorities

3.1 Which authorities should be registered first?

(1) **In the area of Public Documents it is important to first set up / register the "Central authority" of Member States**, or in case there are multiple ones the "Central authorities" of the country.

Based on Art. 15 of Regulation EU 2016/1191, MS have to designate at least one central authority and as per Art 22 (1) point (a) of the Regulation MS shall communicate which is their central authority (or which are their central authorities) together with the relevant contact details.

The registration of central authorities in IMI itself is understood as the communication of the central authorities and their contact details. I.e. by registering the central authorities in the IMI System, Member States clearly comply with this obligation.

(2) After registering / setting up the central authorities, **as a second step Member States should proceed with setting up those authorities** (if in addition to the central authority(ies) there would be any) **that will have a monitoring / supervisory or approval role in the area of Public Documents.**

(3) Once the central authorities and the additional "supervisory" authorities are set up, **registration should continue with setting up additional authorities that are/will be responsible for uploading models of public documents and anonymised samples of forged documents to the IMI repositories.**

I.e. the IMI repository module is made available as of August 2018 and during the first implementation phase the repositories need to be sufficiently populated with information to avoid any unnecessary requests for information at a later stage.

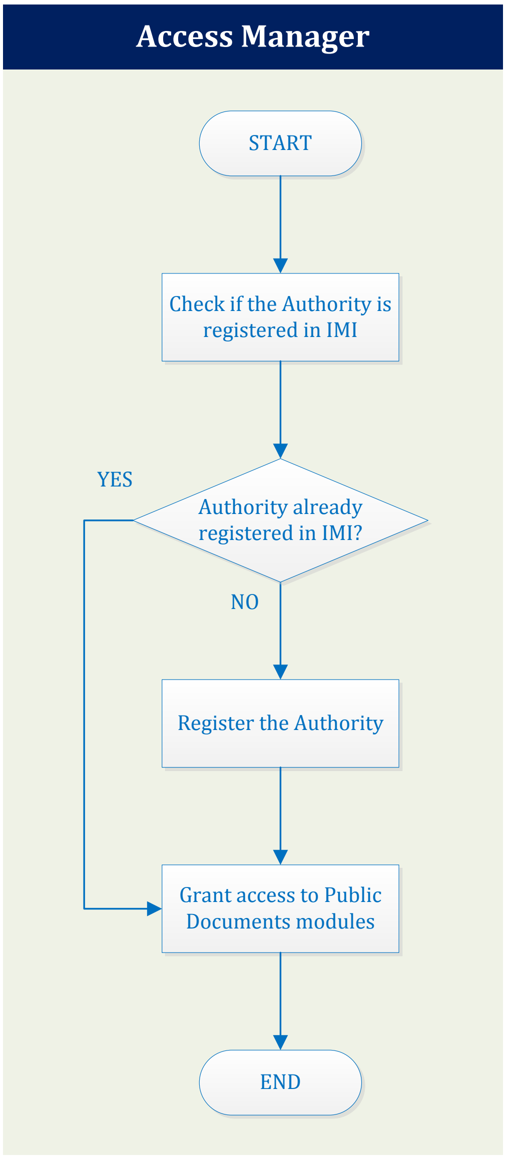
(4) The registration of further authorities afterwards can and should take place in a gradual approach where, considering the needs of their authorities, Member States' IMI Access managers ensure that the authorities that will need to regularly use IMI for checking the authenticity of public documents get their access to the system.

Considering that, depending on the countries administrative structure, potentially a very large number of authorities will need to be registered / set up in IMI, Member States might also opt for:

- a need-based IMI registration process where competent authorities, which are expected to be occasional users, only get registered when a concrete need to check a foreign public document arise.
- a set-up where the central authority(ies) in at least in the initial implementation phase will act in IMI on behalf of other authorities that are expected to check foreign public documents only occasionally.

(Note that this latter option might not be possible due to national legal acts, i.e. in some MS authorities might not at all be allowed to "act on behalf" of other authorities.)

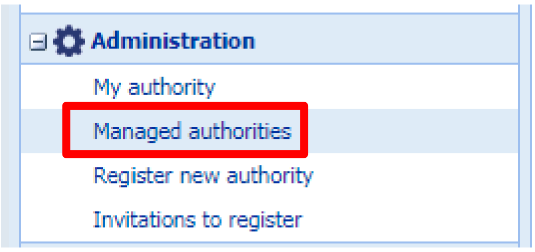
3.2 Overview of the steps for setting up new IMI authorities


Access Manager
START
Check if the Authority is registered in IMI
YES
Authority already registered in IMI?
NO
Register the Authority
Grant access to Public Documents modules
END

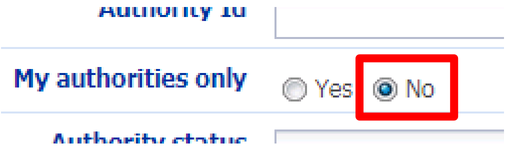
3.2.1 STEP 1 - Checking if the Authority is registered in IMI

When you start to set up authorities in IMI, you will first need to check whether the authority is already registered in the system. **This step is of utmost importance in the area of Public Documents**, where several Member States have planned to register a very high number of competent authorities, including municipalities, local and regional government offices. In many countries, such authorities have already been registered for other IMI modules, in particular in the area of Services and Public procurement. To check whether authorities have or have not been previously registered in IMI:

1. Click the **Administration** menu option on the left, then **Managed authorities**:



2. In the **My authorities only** search criteria, select **No**



Authority Id

My authorities only ○ Yes ● No

Authority status

You may use some additional search criteria, e.g. **Email** (recommended) or **Authority name** field.

Both search criteria allow for searching with a short string of characters, i.e. for example in the e-mail address field it is sufficient to enter @europa.eu

3. Click **Search** on the top right hand toolbar.

4. The list of the authorities matching your criteria will appear:

- **If you find the authority, it means that it is already registered in IMI: follow the instruction from STEP 3 Granting access to Public Documents modules**.
- If you do not find the authority, it means that you have to register a new authority in IMI: follow the instructions in the next step (STEP 2).

The structure of authorities in IMI shall reflect reality, and in this sense competent authorities should not be registered multiple times in the system. In real life, physical authorities are single authorities (two or more competent authorities do not share exactly the same name), thus in IMI authorities should only be registered once.

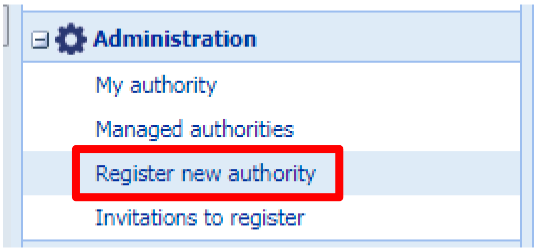
Duplicate registration of authorities, by all means, should be avoided. The IMI Helpdesk will remove (merge) duplicate authorities without prior notice, unless the Member State concerned consulted the Helpdesk beforehand and justified the need for re-registering a competent authority.

In general, you never need to create duplicate authorities: the flexibility of IMI allows users in the same authority to have access rights for different modules, i.e. one user may have access to Public documents modules, while another to the modules related to the Services Directive or to Information Request in the area of Professional Qualifications.

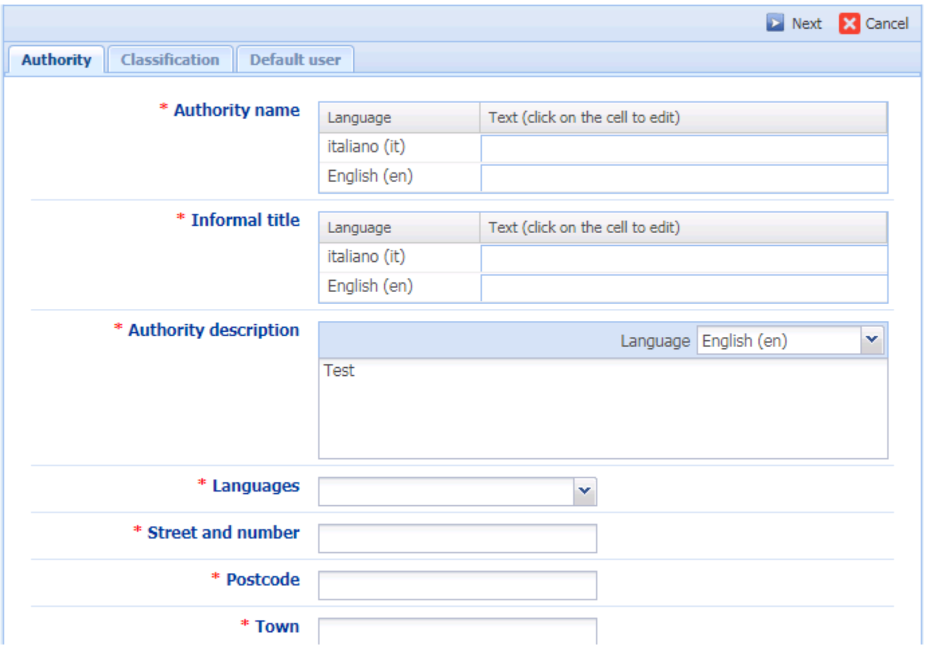
3.2.2 STEP 2 Registering a New Authority in IMI

If the authority is not yet registered in IMI, you will have to do it now. To do so:

1. Click the **Administration** menu option on the left, then **Register new authority**:



2. You are now in the Authority tab. You should see the following screen, where information is displayed on 3 pages:



* Authority name

Language	Text (click on the cell to edit)
italiano (it)	
English (en)	

* Informal title

Language	Text (click on the cell to edit)
italiano (it)	
English (en)	

* Authority description

Language: English (en)

Test

* Languages

* Street and number

* Postcode

* Town

Fill in the data of the authority, then click on **Next** on the top right hand toolbar.

Should you need to collect information from the authorities for their registration, consider using forms provided in the annex of this document (English only).

3. You are now in the Classification tab, where you can select one or more keywords from the following lists:

   - Geographical coverage
   - Authority type

   Make sure that you select at least one keyword from any of the lists, e.g. the geographical coverage list. Click on **Next** on the top right hand toolbar.

4. You are now in the Default user tab. Fill in the details of a user to be registered, then click on **Finish** on the top right hand toolbar.

- When filling in the details of the user, the system will generate a username automatically. If you do not like the system generated username you can change it.

  The system will allow you to save the updated username, unless there is already an IMI user who has the same username.

  The registered user will receive an e-mail about the registration and in 24 hours he/will receive a second e-mail that will include his/her temporary password. Note that **you need to communicate the username to the user outside IMI**, since for security reasons it is not included in the automatic e-mails. For further details concerning the registration of users see section 4.1 of this document

  Note that **the e-mail address of the user has to be unique**, i.e. you cannot register any user with an e-mail address that is already recorded in IMI.

  For security and data protection reasons, the e-mail address registered for a user must be the user's professional personal e-mail address and should not be the address of any shared or functional mailbox.

> It is recommended to have easy-to-remember usernames. IMI Users may wish to have the same username that they have in other IT Systems or for other IT applications used in their office. Should this be the case they can "reuse" their username as long as that has not been assigned yet to another IMI user.

The new authority is now registered in the system. The system will now remind you to grant to the authority access to the relevant IMI modules (administrative procedures, in which the authority will be involved). To do so, refer to the next step.

3.2.3 STEP 3 Granting access to Public Documents modules

Depending on the responsibilities of the authority you are setting up in IMI, you may wish to grant access to only one or both of the Public Documents modules:

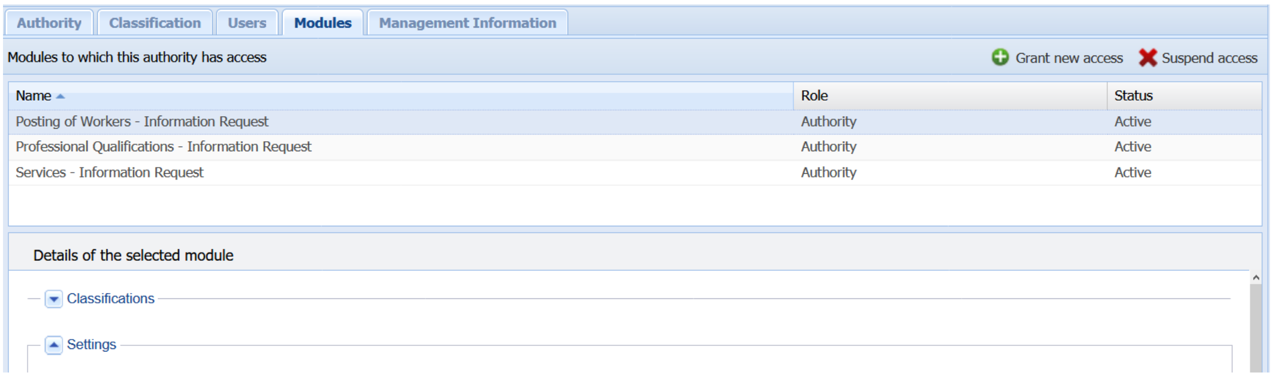
- **Public Documents - Repositories** (models of documents and samples of forged documents)
- **Public Documents - Request for information** (concerning the authenticity of documents)

> If necessary and relevant, Access managers can also grant these accesses to their own authority. This could be useful e.g. if a NIMIC would be involved in future in closely monitoring the MS's activity in these modules.
>
> Should they wish to do so, they need to open their authority's details through the **Administration** menu option. The simplest way to open the details is to select the **My authority** sub menu item, but it is also possible via the Managed authorities search (as described in section 3.1). For instructions on how to grant access see the following sections.

3.2.3.1 Granting access to the Public documents repository

1. Go to the Modules (4th) tab of the authority details.

   - If you have just completed the registration of a new authority, IMI will automatically take you there and you will see the list of modules empty.
   - If you are granting access to a previously registered authority, you will see the list of modules to which the authority already has access.



Modules to which this authority has access

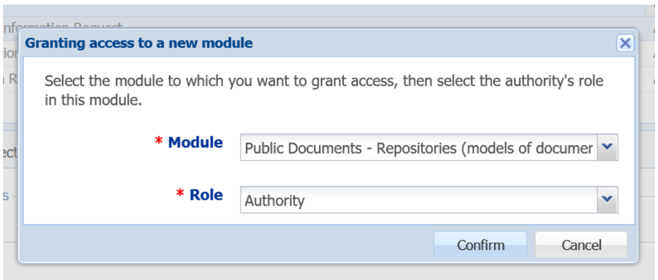
Name	Role	Status
Posting of Workers - Information Request	Authority	Active
Professional Qualifications - Information Request	Authority	Active
Services - Information Request	Authority	Active

Details of the selected module

2. Click on **Grant new access** on the top right hand toolbar

3. In the pop-up window select:

   - **Module: Public Documents - Repositories (models of documents…)**
   - **Role: Authority** *(for the repository module only this role is available)*



Granting access to a new module

Select the module to which you want to grant access, then select the authority's role in this module.

* Module: Public Documents - Repositories (models of documer

* Role: Authority

4. Click **Confirm**.

5. You are now on a page, where you have to

   - select one or more keywords in the **Classification** section that describe the competencies/responsibilities of the authority in this module.

     The selected keywords will be used in the authority searches. The keywords available for selection are:

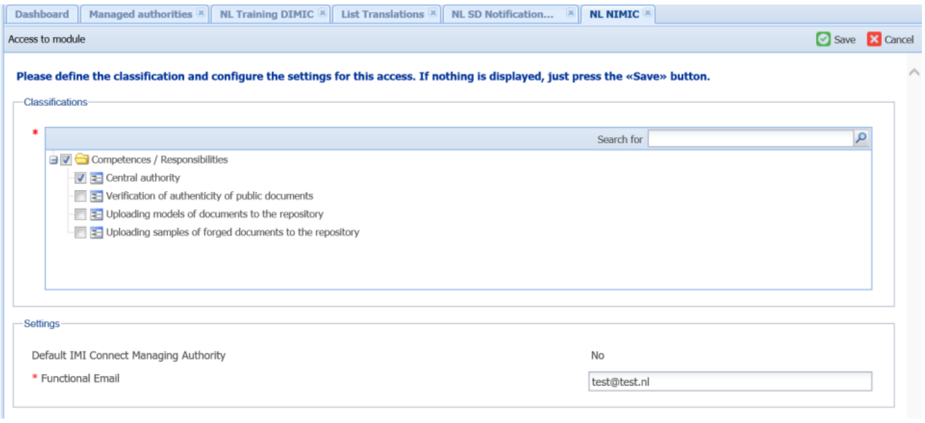
     - *Central authority*
     - *Verification of authenticity of public documents*
     - *Uploading models of documents to the repository*
     - *Uploading samples of forged documents to the repository*

     In case of the Central authority(ies) of your Member States you must select the Central authority *in the classification section.*

   - enter an e-mail address in the **Functional Email** field.

     In this field you should enter the e-mail address of a functional mailbox to which any repository related e-mails should be sent. For this module only a limited number of automatic e-mails will *be sent, mainly when new versions of a repository entry are activated. If the authority does not have a functional e-mail address or if for any reason you wish to do so, you may also enter the e-mail address of a user in the field.*

The e-mail address in this field does not need to be unique, any previously recorded e-mail address can be reused.



Access to module

Please define the classification and configure the settings for this access. If nothing is displayed, just press the «Save» button.

Classifications

*

☑ Competences / Responsibilities
- ☑ Central authority
- □ Verification of authenticity of public documents
- □ Uploading models of documents to the repository
- □ Uploading samples of forged documents to the repository

Settings

Default IMI Connect Managing Authority: No

* Functional Email: test@test.nl

6. Click on **Save** on the top right hand toolbar.

3.2.3.2 Granting access to the Public documents – Public Documents - Request for information (concerning the authenticity...)

For this module, it is important that you first grant access to those authorities which should have a monitoring / supervisory or approval role for the exchanges of information concerning the authenticity of Public Documents. These authorities will need to have a **Coordinator role for the module.** In case you would like all your authorities to exchange information without any sort of supervision, they should all have a coordinator role for this module.

You should proceed with granting access to the supervised/monitored authorities only after setting up the coordinators of this module. The following sections will explain how to do so.

In the exceptional case when a Member State only registers one authority (the Central authority as per the regulation) for the area of Public Documents, that authority must be assigned a coordinator role.

For the information request module, Member States must have at least one authority registered with a coordinator role.

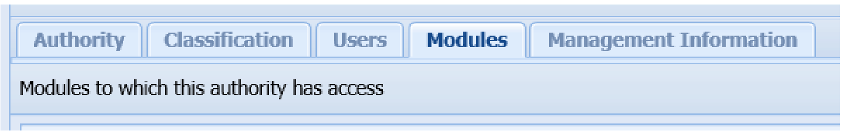
Note that **the form to exchange information concerning the authenticity of documents will only be active in IMI as of 16th February 2019** (as of when, according to the Regulation, authorities should start exchanging information). Prior to this date, IMI is only open for setting up/registering authorities for the module.

A) Granting access with a Coordinator role

Coordinators are will be able to do everything in IMI that an "Authority" can do. I.e. If an authority will be acting both as a coordinator and as an authority in IMI, it only needs to be set up once with a coordinator role.

IMI authorities that are assigned a coordinator role for the request module can monitor and, if needed, supervise the requests of those authorities to which they are linked.

1. Stay on/go to the Modules (4th) tab of the authority details.

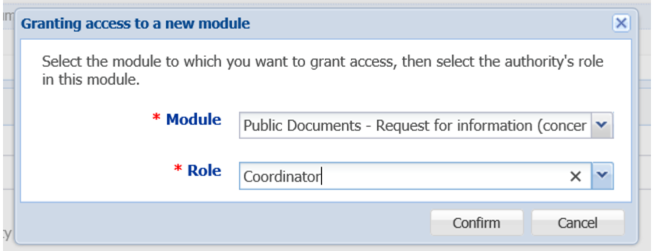


Modules to which this authority has access

2. Click on **Grant new access** on the top right hand toolbar

3. In the pop-up window select:

   - **Module: Public Documents - Request for information** (concerning the authenticity…)
   - **Role: Coordinator**



Granting access to a new module

Select the module to which you want to grant access, then select the authority's role in this module.

* Module: Public Documents - Request for information (concer

* Role: Coordinator

4. Click **Confirm**.

5. You are now on a page, where you have to:

   ○ select one or more keywords in the **Classification** section that describe the competencies/responsibilities of the authority in this module.

   The selected keywords will be used in the authority searches. The keywords available for selection are:

   - *Central authority*
   - *Responsible for transmission of requests*
   - *Verification of authenticity of public documents*
   - *Coordination of incoming requests*
   - *Coordination of outgoing requests*
   - *Sending requests to verify the authenticity of documents*
   - *Responding to requests concerning the authenticity of documents*

   ***In case of the Central authority(ies) of your Member States, you must select the Central authority** in the classification section. In addition, if your MS has multiple central authorities you should select **Responsible for transmission of requests** as a keyword for the central authority that will have this responsibility.*

- customize the **settings** for the coordinator according to your needs (note that you may not need to change any of the default settings):

Setting	Options	Effect	Remarks
Does the Coordinator participate in the referral process?	**Yes**	In case of a disagreement between the sender and recipient of the request the coordinator will be able to give its opinion	***Default setting***
	No	In case of a disagreement between the sender and recipient of the request the coordinator will not be able to give its opinion	-
Does the Coordinator wish to approve Competent Authority requests before they are sent?	**Yes**	When a linked authority sends a request, the Coordinator will have to approve the request before it gets sent to the recipient in the other MS. The coordinator will not need to approve requests of those authorities that are not subject to approval.	*For the authorities that should send requests only with their coordinator's approval, the 'Subject to approval' flag has to be set to Yes.*
	No	The coordinator will never be involved in approving requests of other authorities.	***Default setting***
Does the Coordinator wish to approve Competent Authority replies before they are sent?	**Yes**	When a linked authority responds to a request, the Coordinator will have to approve the reply before it gets sent to the other MS. The coordinator will not need to approve replies of those authorities that are not subject to approval.	*For the authorities that should only respond to requests with their coordinator's approval, the 'Subject to approval' flag has to be set to Yes.*
	No	The coordinator will never be involved in approving replies of other authorities.	***Default setting***

- enter an e-mail address in the **Functional Email** field.

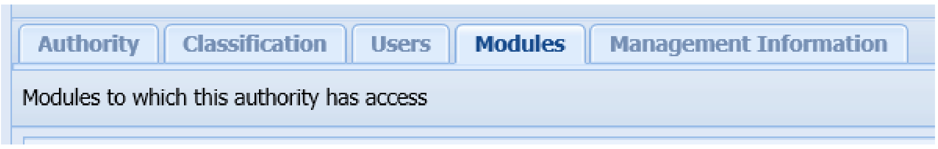
  In this field you should enter the e-mail address of a functional mailbox to which any repository related e-mails should be sent. For this module only a limited number of automatic e-mails will be sent, mainly when new versions of a repository entry are activated. If the authority does not have a functional e-mail address or if for any reason you wish to do so, you may also enter the e-mail address of a user in the field.

  The e-mail address in this field does not need to be unique; any previously recorded e-mail address can be reused.

6. Click on **Save** on the top right hand toolbar.

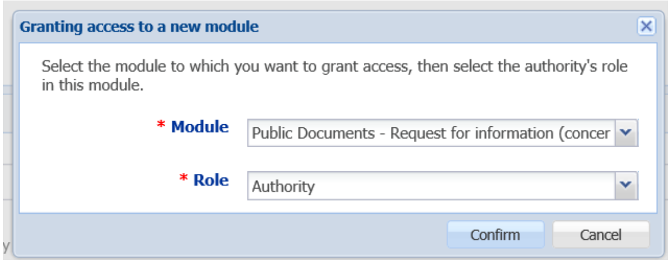
B) Granting access with an Authority role

1. Stay on/go to the Modules (4th) tab of the authority details.



Modules to which this authority has access

2. Click on **Grant new access** on the top right hand toolbar
3. In the pop-up window select:
   - **Module: Public Documents - Request for information** (concerning the authenticity…)
   - **Role: Authority**



Granting access to a new module

Select the module to which you want to grant access, then select the authority's role in this module.

* Module: Public Documents - Request for information (concer

* Role: Authority

4. Click **Confirm**.

5. You are now on a page, where you have to:

   - select one or more keywords in the **Classification** section that describe the competencies/responsibilities of the authority in this module.

     The selected keywords will be used in the authority searches. The keywords available for selection are:

     - *Central authority*
     - *Responsible for transmission of requests*
     - *Verification of authenticity of public documents*
     - *Coordination of incoming requests*
     - *Coordination of outgoing requests*
     - *Sending requests to verify the authenticity of documents*
     - *Responding to requests concerning the authenticity of documents*

- customize the **settings** for the authority according to your needs (note that you may not need to change any of the default settings):

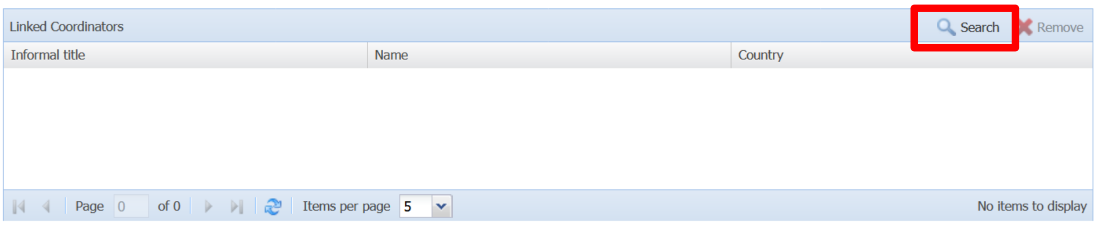
Setting	Options	Effect	Remarks
Is this Authority subject to approval by the Coordinator before sending request and replies?	**Yes**	When the authority sends a request or a reply, the Coordinator will have to approve it before it reaches the intended recipient.	*For this setting to work, the coordinators have to set the Approve request/approve replies flags to Yes*
	No	The authority does not need it's coordinator's approval neither for sending requests nor for responding to received requests	***Default setting***
Is this Authority exceptionally allowed to refuse requests on behalf of its Member State?	**Yes**	The Authority is allowed to refuse incoming requests on behalf of its Member State	*The intention to refuse requests needs to be communicated to the IMI Helpdesk via the NIMIC*
	No	The authority needs to accept the incoming requests and then respond to it. When replying it can obviously indicate if information is not available or the authenticity of a document for any reason could not be verified.	***Default setting***
Is this authority allowed to accept incoming requests?	**Yes**	The authority can be contacted directly by authorities of other Member States (i.e. can receive incoming requests)	***Default setting***
	No	The authority cannot receive requests directly from other Member States. It can only receive requests forwarded by another authority of its own country, e.g. by the central authority,	*This setting should be set to No, if MS would like to centralise incoming requests. Note that those authorities who have a coordinator role for this module will always be able to receive requests from other countries*

- enter an e-mail address in the **Functional Email** field.

  In this field you should enter the e-mail address of a functional mailbox to which any repository related e-mails should be sent. For this module only a limited number of automatic e-mails will be sent, mainly when new versions of a repository entry are activated. If the authority does not have a functional e-mail address or if for any reason you wish to do so, you may also enter the e-mail address of a user in the field.

  The e-mail address in this field does not need to be unique; any previously recorded e-mail address can be reused.

6. Now you have to select the Linked Coordinator for the authority. Click on the Search button in the linked coordinators box of the settings section (box below the Functional Email field):

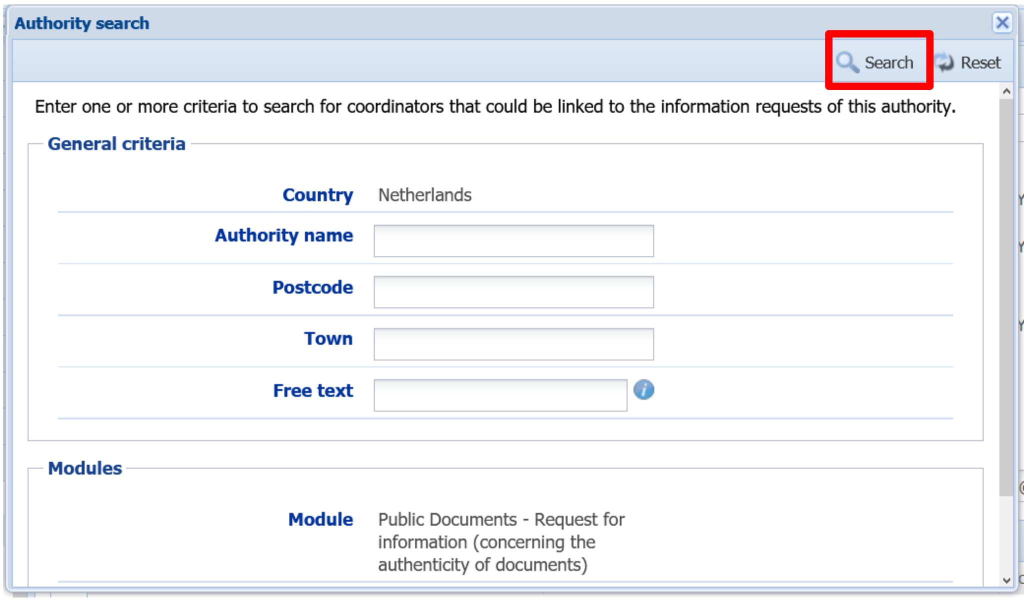


Linked Coordinators

Informal title	Name	Country

Page 0 of 0 · Items per page 5 · No items to display

7. You can use the general criteria in the Authority search panel to find the authority that will act as coordinator, but since it is unlikely that there will be many coordinators in the module, you do not necessarily need to set any criteria, but simply click on Search in the pop-up:



Authority search

Enter one or more criteria to search for coordinators that could be linked to the information requests of this authority.

General criteria

Country: Netherlands

Authority name:

Postcode:

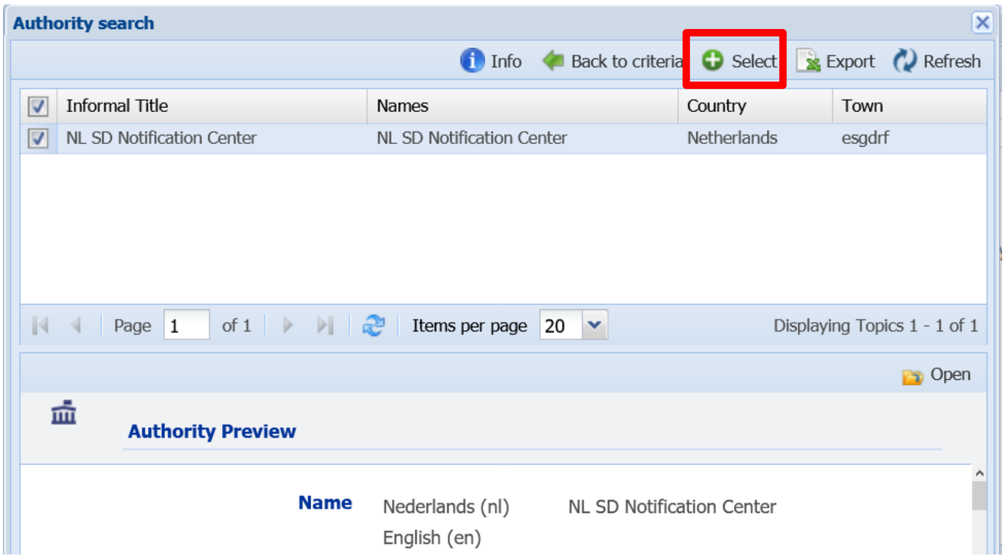
Town:

Free text:

Modules

Module: Public Documents - Request for information (concerning the authenticity of documents)

8. In the results list, select the coordinator(s) that should be supervising/monitoring or, if an active approval process is in place, approve the authorities requests in the module, and click **Select**:



Authority search

☑	Informal Title	Names	Country	Town
☑	NL SD Notification Center	NL SD Notification Center	Netherlands	esgdrf

Page 1 of 1 · Items per page 20 · Displaying Topics 1 - 1 of 1

Authority Preview

Name: Nederlands (nl) NL SD Notification Center
English (en)

9. The authority has been added as Linked Coordinator. Click on **Save** on the top right hand toolbar.

4 Registering users and user management

When registering a new authority you always need to register one user as part of the registration process (see Point 4 in Section 3.2.2). This user by default will receive an Administrator right for his/her own authority's data and users and all basic roles for the modules to which you have granted access after the registration.

4.1 Registering additional users

1. Go to the **Users** tab of the registered authority to see the existing user(s) of the authority

2. Register additional users by clicking on **Add user.**

   - When filling in the details of the user, the system will generate a username automatically. If you do not like the system generated username you can change it.

     The system will allow you to save the updated username, unless there is already an IMI user who has the same username.

     The registered user will receive an e-mail about the registration and in 24 hours he/will receive a second e-mail that will include his/her temporary password. Note that **you need to communicate the username to the user outside IMI**, since for security reasons it is not included in the automatic e-mails.

     Note that **the e-mail address of the user has to be unique**, i.e. you cannot register any user with an e-mail address that is already recorded in IMI.

     For security and data protection reasons, the e-mail address registered for a user must be the user's professional personal e-mail address and should not be the address of any shared or functional mailbox.

     > ☝ It is recommended to have easy-to-remember usernames. IMI Users may wish to have the same username that they have in other IT Systems or for other IT applications used in their office. Should this be the case they can "reuse" their username as long as that has not been assigned yet to another IMI user.

   - In the **Roles** box of the page you can select the roles/rights that the new user should have:

     - **Administrator** rights, which will allow him/her to manage the data and the user of his/her won authority, including resetting passwords for his/her colleagues. If an authority has a large number of users, the **Administrator** role should not be given to all users, but only to selected ones.
     - **Handler** rights, i.e. he can create repository entries or deal with requests
     - only **Viewer** rights in a module, i.e. he/she will only be able to see the repositories and requests

     If the authority has a coordinator role for the information request module, a user may also be given:

     - **Approver** rights, i.e. will be responsible for monitoring/supervising and in case of an activated approval process approve requests and replies

     It is possible to give users rights for some modules only and not for all of them, e.g. to decide that only some users will be allowed to deal with requests.

     Note that at least one user in the authority will need to have:

- **Administrator** role
- **Handler** role
- In case of coordinators of the request module: **Approver** role

It is not mandatory to have viewers

> If you were granting access to a previously registered authority, the users who had Administrator right in that authority automatically receive user roles for the new modules. Should you wish to remove their rights for the Public Documents module, please Edit their details (See following section).

4.2 Usernames, temporary passwords and first login to IMI

Usernames for all users must be communicated outside the system. Usernames are not included in any automatic e-mail sent from IMI.

- **Temporary passwords for newly registered users** are sent 24 hours after their registration.
- **Temporary passwords in case of password reset** are sent out by the system with no more than 15 minutes delay

If, for any reason, a newly registered user needs to urgently log onto IMI, his/her password can be reset immediately after registration. In this case, a temporary password will arrive in 15 minutes. Note that in this case the 24 hours delayed e-mail with the "first" temporary password should be simply ignored.

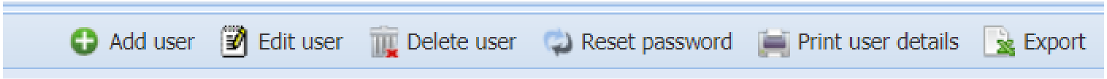
With the username and the temporary password users will be able to logon to IMI. When first logging on, they will have to set their personal password and 12 digit security code. Users should consider the following recommendations:

- **When logging on with a temporary password, it is important to enter the username and the temporary password manually**, even if the fields on the login screen are prefilled. If then the browser asks if you would like it to store your password you have to answer NO.
- Users first have to complete the logon process with the temporary password (set your password and security code). If they would like the browser to retain their password, they have to log out and login once again with the newly set password. Again they should first enter the username and newly set password manually. This time the browser will ask again if they would like it to store/remember the password. This time the answer can be YES.
- **The usernames, passwords and security codes in IMI are case sensitive**, and you always have to pay attention to correctly enter capital characters.
- It is strongly recommended to enter temporary passwords manually in order to avoid the unfortunate mistake of copying additional characters in front of or after the password.
- **The temporary passwords always consist of 2 capital letters + 4 small case characters + 2 numeric characters** (I.e. the first two letter are always capital letters – this is important as a capital O can easily be confused with a number 0 or a small case l can easily be confused with a capital I)
- **The temporary passwords can only be used for a one-off login.** When logging on with a temporary password users need to set first a personal password and then a security code for themselves. (For ease of use you may consider recommending the setting up a simple security code that still meets the rules – these will be easy to enter for subsequent logins)

4.3 Editing and deleting registered users, resetting passwords

Users can be managed on the **Users tab** of the authorities, if the details of an authority are opened from the Administration / Managed authorities menu option.

An authority's own Administrator can also manage the users of his/her own authority on the Users tab, via the Administration/My authority menu option.



The registered users of the authority are displayed in a list. To manage a user, select the user in the list and click on

- **Edit user** – if you would like to modify any detail or the rights of a registered user.
- **Reset password** – if you would like to reset the password of a user
- **Delete user** – if you would like to delete a registered user. (Users who no longer need access to IMI should be deleted from the system without any delay)

You can also **print** the details of a registered user or **export** the list of users registered for the authority using the corresponding buttons.

5 After the Registration

5.1 Updating the data of registered authorities

To update the data of a registered authority, Administrators in Access Managers simply have to:

- open the details of the authority from **the Administration / Managed authorities** menu option
- on the first **Authority** page, click on the **Edit authority** button
- make the necessary changes and the click on **Save**.

To update keywords, settings or the functional mailbox registered for a module the same steps should be followed. **After clicking on the Edit button** on the first page you should go to the **Modules** tab. In the list of Modules you have to select the module for which the data should be updated and then make the necessary change.

5.2 Suspending accesses and deactivating a registered authority

When an authority no longer needs to have access to an IMI module, the access can and should be suspended. This can be done following the steps below:

- open the details of the authority from the **Administration / Managed authorities** menu option
- go to the Modules tab and in the list of modules select the one to be suspended
- Click on the **Suspend access** button, justify the suspension briefly and **confirm**

Note that you may not be able to suspend the access if e.g. the authority is involved in open requests, is responsible for active repository entries or is a coordinator of other authorities. If the system does not allow you to suspend the access, please contact the IMI Helpdesk for support.

When all accesses of an authority are suspended, and if the authority should no longer have access to IMI, the authority should be deactivated. The button to **Deactivate** an IMI authority is available on the first authority tab of the detailed view of the authority. (Note that the button is not visible in Edit mode.).

You can only deactivate an authority after you have suspended all its accesses. After clicking on the **Deactivate authority** button, you will have to justify and confirm the action in a pop-up window.

You may not be able to deactivate an authority if e.g. the authority is involved in open requests, is responsible for active repository entries or is a coordinator of other authorities. If the system does not allow you to deactivate the authority, please contact the IMI Helpdesk for support.

6 Further support

Let us know if we can be of any further assistance or if you have any questions:

National IMI Coordinators:

http://ec.europa.eu/internal_market/imi-net/contact/index_en.htm

IMI website:

http://ec.europa.eu/internal_market/imi-net/

IMI helpdesk:

imi-helpdesk@ec.europa.eu

Annex I – Registration forms

PUBLIC DOCUMENTS REPOSITORY &
PUBLIC DOCUMENTS – REQUEST FOR VERIFYING AUTHENTICITY OF DOCUMENTS

REGISTRATION FORM
- FOR NEW AUTHORITIES TO BE REGISTERED IN IMI -

I. GENERAL INFORMATION ABOUT THE COMPETENT AUTHORITY*

Official Authority Name* *(where it exists please provide this in all the official languages of the Member State concerned)*	
Informal Title[1]* *(to be translated for other Member States)*	
Authority description* *(Give a brief description of your authority, its competences and responsibilities. This data will be translated for other Member States)*	
Languages understood by the authority's users	

II. CONTACT DETAILS OF THE AUTHORITY*

Street*	
Postcode*	
Town*	
Region/Area	
Country*	
Telephone number*	
Fax number	
E-mail address* *(Ensure that this is an e-mail address that will be regularly checked by your authority. It will be used for important communication from IMI to the authority.)*	
Web site address	

[1] The **Informal title** should convey the role of the authority in a clear and unambiguous manner to help other users understand the nature of the authority. It will be translated into all EU languages.

III. PLEASE INDICATE THE GEOGRAPHICAL COVERAGE AND THE TYPE OF THE AUTHORITY

□ National □ Regional □ Local

□ Competent Authority

□ IMI Coordinator with federal responsibility

□ IMI Coordinator with national responsibility

□ IMI Coordinator with regional responsibility

IV. INFORMATION ABOUT THE FIRST USER TO BE REGISTERED IN THE AUTHORITY*

First Name*	
Surname*	
Default language*	
E-mail address*	
Telephone number	

V. INFORMATION ABOUT ADDITIONAL USERS THAT SHOULD BE REGISTERED FOR THE AUTHORITY

TO BE FILLED IN ONLY IF THE AUTHORITY ALREADY NOMINATED MORE THAN ONE USER

*First Name**	
*Surname**	
*Default language**	
*E-mail address**	
Telephone number	

*First Name**	
*Surname**	
*Default language**	
*E-mail address**	
Telephone number	

VI. THE AUTHORITY'S ACCESS TO THE PUBLIC DOCUMENTS MODULES*

Please select the IMI module to which the authority should have access

□ Public Documents - Repositories (models of documents and samples of forged documents)

□ Public Documents - Request for information (concerning the authenticity of documents)

Please indicate the role that should be assigned to the authority for requests in the *Public documents – Request for verifying authenticity of documents* module

□ Authority □ Coordinator

The Coordinator role should be assigned to authorities, which are responsible for monitoring requests in the area. If a MS only has one authority responsible for this module it should be assigned a Coordinator role.

VII. RESPONSIBILITY(IES)/COMPETENCY(IES) OF THE AUTHORITY

Please select the keyword that describes best the responsibility(ies) of the authority*

'Public Documents - Repositories (models of documents and samples of forged documents)' module

□ Central authority

□ Verification of authenticity of public documents

□ Uploading models of documents to the repository

□ Uploading samples of forged documents to the repository

'Public Documents - Request for information (concerning the authenticity of documents)" module

□ Central authority

□ Responsible for transmission of requests

□ Verification of authenticity of public documents

□ Coordination of incoming requests

□ Coordination of outgoing requests

□ Sending requests to verify the authenticity of documents

□ Responding to requests concerning the authenticity of documents

PLEASE NOTE THAT THE CLASSIFICATION OF THE AUTHORITY WITH THE ABOVE KEYWORDS WILL NOT HAVE ANY IMPACT ON THE HANDLING OF REQUESTS. THIS IS TO BE SEEN ONLY AS DESCRIPTIVE INFORMATION ABOUT THE AUTHORITY, WHICH CAN BE CHANGED AT ANY STAGE. THE OBJECTIVE OF THE CLASSIFICATION IS TO FACILITATE THE SEARCH AMONG AUTHORITIES IN IMI.

PUBLIC DOCUMENTS REPOSITORY & PUBLIC DOCUMENTS – REQUEST FOR VERIFYING AUTHENTICITY OF DOCUMENTS

REGISTRATION FORM
- FOR AUTHORITIES ALREADY REGISTERED IN IMI –

I. GENERAL INFORMATION ABOUT THE COMPETENT AUTHORITY*

Official Authority Name (as it is registered in IMI)	

II. THE AUTHORITY'S ACCESS TO THE PUBLIC DOCUMENTS MODULES*

Please select the IMI module to which the authority should have access

□ Public Documents - Repositories (models of documents and samples of forged documents)

□ Public Documents - Request for information (concerning the authenticity of documents)

Please indicate the role that should be assigned to the authority for requests in the *Public documents – Request for verifying authenticity of documents* module

□ Authority □ Coordinator

The Coordinator role should be assigned to authorities, which are responsible for monitoring requests in the area. If a MS only has one authority responsible for this module it should be assigned a Coordinator role.

III RESPONSIBILITY(IES)/COMPETENCY(IES) OF THE AUTHORITY

Please select the keyword that describes best the responsibility(ies) of the authority*

'Public Documents - Repositories (models of documents and samples of forged documents)' module

□ Central authority

□ Verification of authenticity of public documents

□ Uploading models of documents to the repository

□ Uploading samples of forged documents to the repository

'Public Documents - Request for information (concerning the authenticity of documents)" module

□ Central authority

□ Responsible for transmission of requests

□ Verification of authenticity of public documents

□ Coordination of incoming requests

□ Coordination of outgoing requests

□ Sending requests to verify the authenticity of documents

□ Responding to requests concerning the authenticity of documents

PLEASE NOTE THAT THE CLASSIFICATION OF THE AUTHORITY WITH THE ABOVE KEYWORDS WILL NOT HAVE ANY IMPACT ON THE HANDLING OF REQUESTS. THIS IS TO BE SEEN ONLY AS DESCRIPTIVE INFORMATION ABOUT THE AUTHORITY, WHICH CAN BE CHANGED AT ANY STAGE. THE OBJECTIVE OF THE CLASSIFICATION IS TO FACILITATE THE SEARCH AMONG AUTHORITIES IN IMI.

IV. USERS WHO ARE ALREADY REGISTERED IN IMI AND WHO SHOULD HAVE ACCESS TO THE NEW MODULES:

………

V. INFORMATION ABOUT ANY NEW USER(S) WHO SHOULD HAVE ACCESS TO THE MODULES IN IMI

*First Name**	
*Surname**	
*Default language**	
*E-mail address**	
Telephone number	

*First Name**	
*Surname**	
*Default language**	
*E-mail address**	
Telephone number	

FOR ADDITIONAL USERS THE LAST SECTION IS TO BE REPEATED