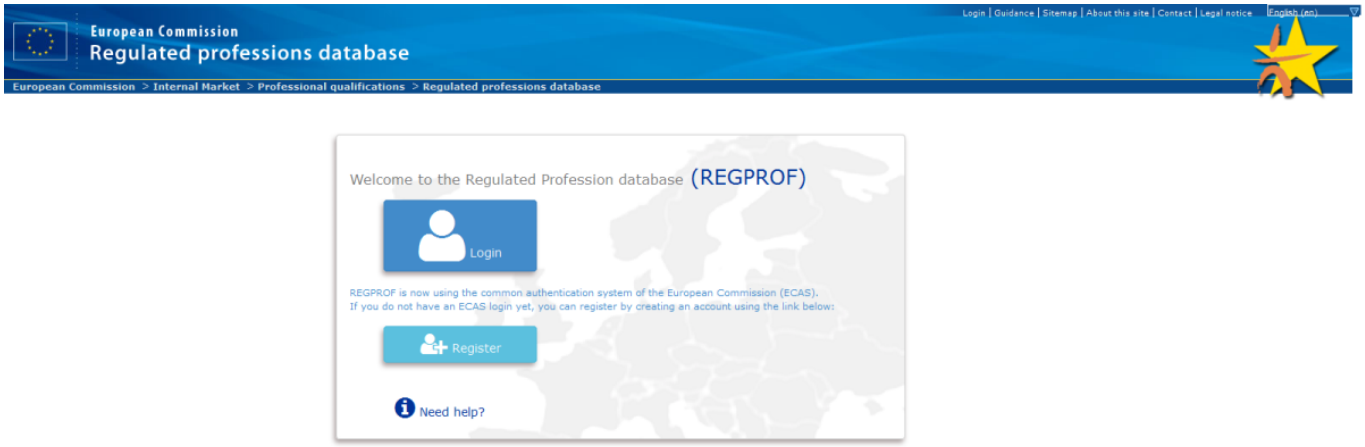
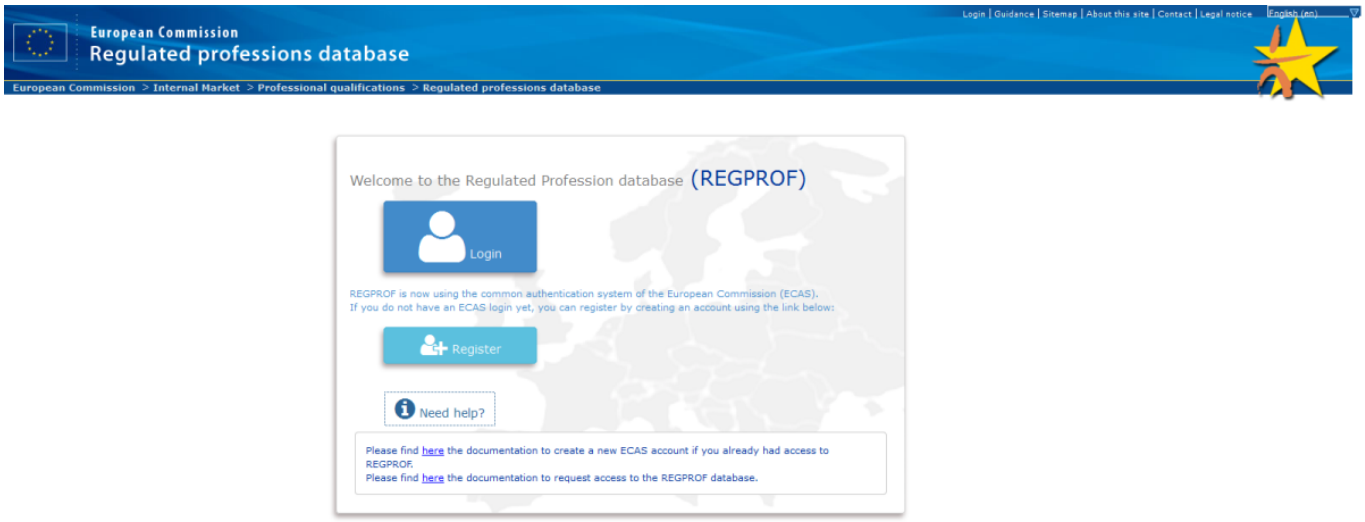
Serviciul de autentificare al Comisiei Europene (ECAS)

0.1 regprof login of register or need help

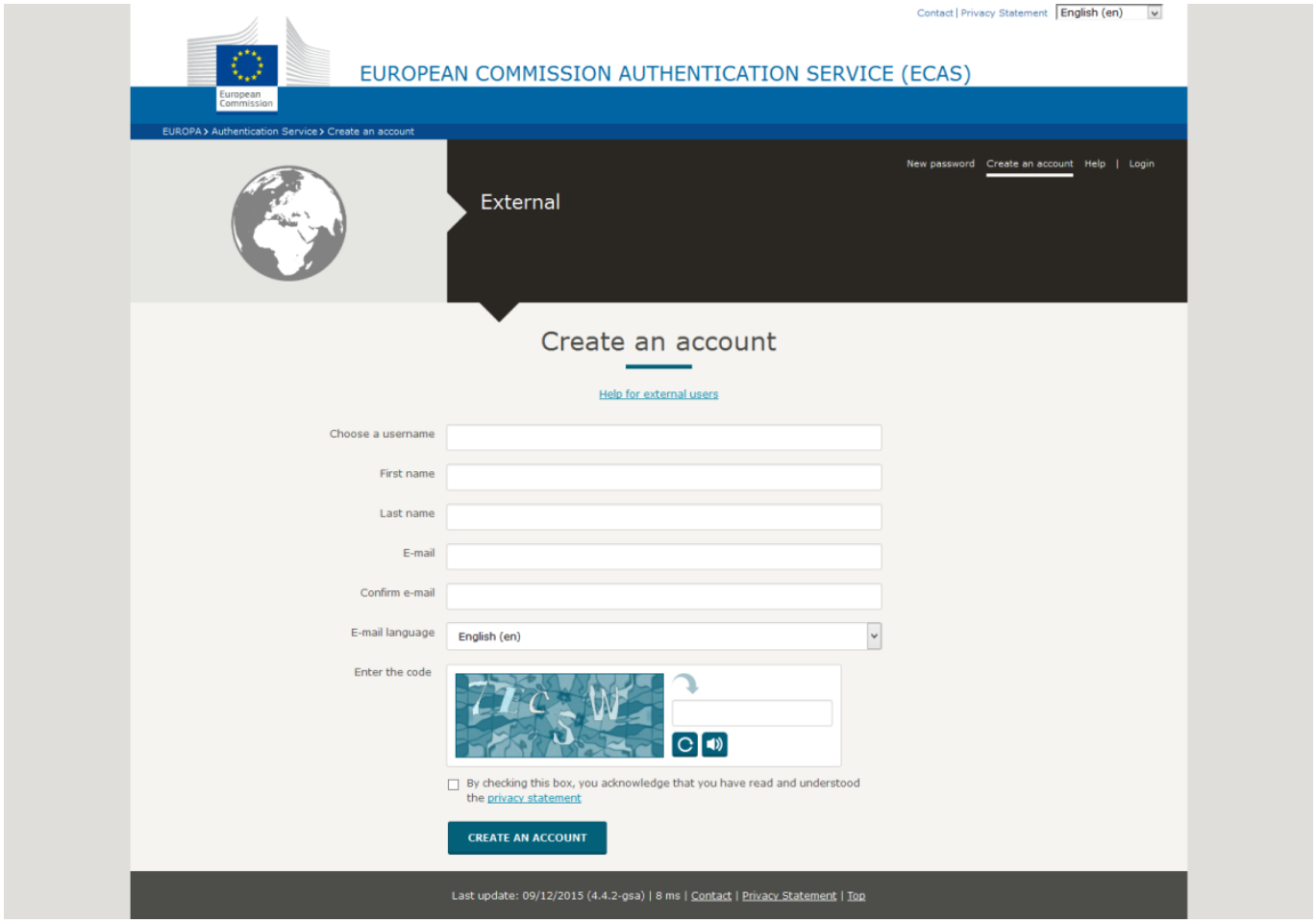


0.2 regulated professions database on December 2015

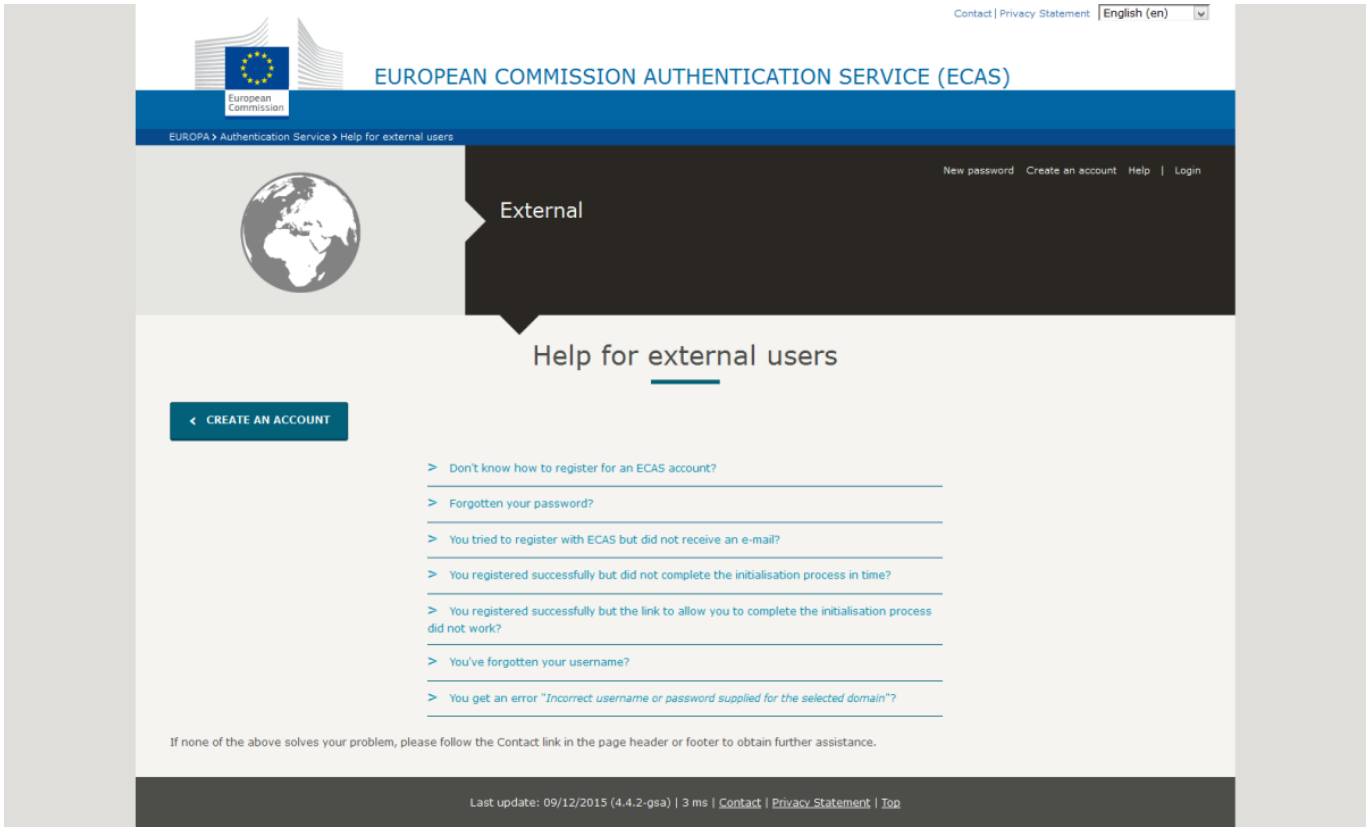
1.0 regprof need help links



2.0 regprof register

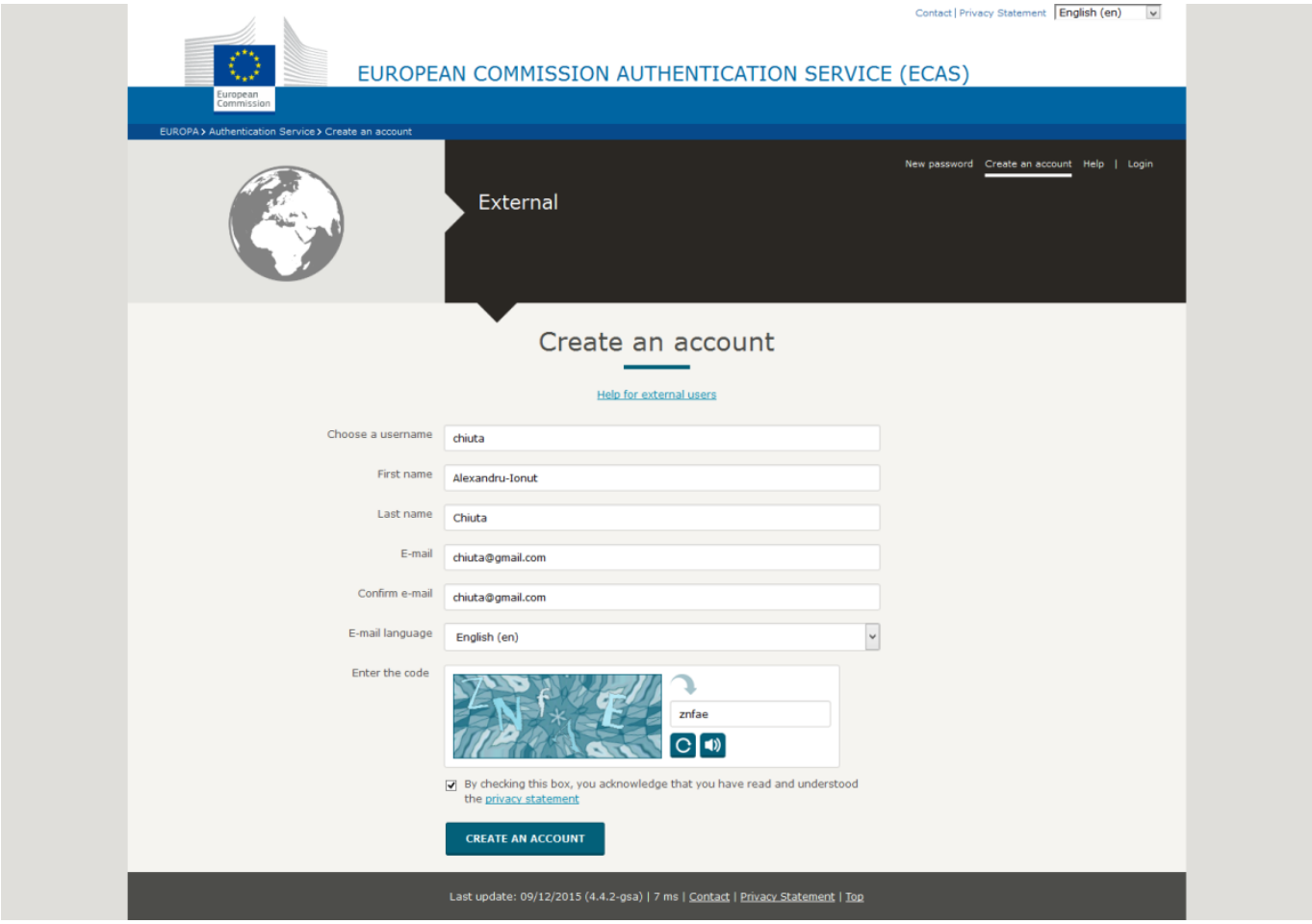


2.1 regprof register help for external users



2.2 regprof register help

2.3 regprof register personal data



2.4 regprof register ec ims privacy statement

EUROPEAN COMMISSION AUTHENTICATION SERVICE (ECAS)

Privacy statement for users registered with the European Commission's Identity Management Service

1. What is the Identity Management Service?

The European Commission's Identity Management Service (IMS) provides a common way for users to register or be registered for access to a number of different Commission information systems or services (referred to hereafter as *sites*).
You are affected by this privacy statement if you use the European Commission Authentication Service (ECAS) when logging into Commission sites, as it means that you have been registered in IMS.

Users include the Commission's own staff, personnel of other organisations and members of the public.
Registration may occur:

- at the initiative of a user or of the organisation that the user belongs to or represents
- by means of an automatic transfer of information from the user's organisation to the Commission
- by means of direct entry of the relevant information by the user

IMS includes facilities for authenticating registered users and controlling their access to Commission sites.

In each case, the personal data that is recorded is governed by Regulation (EC) 45/2001.

IMS falls under the responsibility of the Controller, Mr Stephen Quest, Director General, Informatics DG. Further responsibility lies with each processor of the information.

Individual Commission sites that rely on IMS for commonly required personal data may nevertheless collect additional personal data themselves. This is covered by the sites' own privacy statements.

2. What information do we collect, for what purpose and through which technical means?

In general, registration is required:

- if access to a site is restricted to authorised persons
- if there is a simple need for the site to remember you between visits and adapt itself to your needs or wishes
- to allow you to receive further information that you have requested, such as newsletters and information updates
- to grant you individual privileges that you might request or otherwise be entitled to

We store the information that you provide on the registration form (if you registered yourself) or that your organisation provides directly to us. The information you provide may be made available to Commission sites other than the one for which you originally obtained the account provided that you attempt to access them while logged in using your account. By logging in and accessing accounts you are indicating your consent to the use of the data as described in this statement.

The data obtained from the registration process includes both personal details and, if you are registered as a representative or member of an organisation, details related to your link with that organisation. Personal details include your names, geographical location, areas of interest (with respect to the Commission), e-mail address and telephone number. Concerning your organisation, the details may include its name, the department you work for, your office address, the nature of your relationship with the organisation (e.g. employee), your roles and job title and, in order to avoid creating duplicate records, a unique identifier. Information that is obtained from your organisation is subject to the regulations concerning the transfer of personal data and may be only a subset of that mentioned.

The account that we create contains enough information for us to have reasonable confidence that its subsequent usage is by yourself or someone with access to the information you provided (including the password).

We also store certain additional information (listed below) relating to the activity on the user account that we create for you, so that we can protect both your identity and the integrity of the Commission systems that you access.

The additional information is used to diagnose and resolve problems and to deal with security incidents. Much of it relates to attempts to use an identity and thus to events that occur before a user has successfully authenticated.

The Identity Management Service also stores a list of the access rights granted to you by the Commission for the purpose of granting or denying access to individual sites.

Users can inspect all the data that is maintained about their own account, allowing them to check that their account has not been used, and that attempts have not been made to use it, without their knowledge.

We may collect the following additional data about each user:

- Date and time of
  - most recent successful and unsuccessful authentication
  - last change of password
  - last password reset
- Number of good logins and failed attempts
- Your most recent passwords - to make sure you follow the prevailing security policy regarding password re-use.

When you login and / or change your password, we may record further information in log files, such as the IP address used, in line with the purposes stated above. This information can help in following up any doubtful activity relating to your account. It will **not** be used to monitor your activity, except to allow the removal of the account when no longer used.

Many Commission sites use the European Commission Authentication Service (ECAS) for user authentication: ECAS has a special user interface, independent of the client site and provides a single sign-on experience. Some of the information mentioned here is not relevant for the Commission sites that do not use ECAS – if you never login through ECAS it will therefore not be maintained in your account data. Note that logging in through ECAS always involves a page distinctively marked with the ECAS logo. Each time you login to a site protected by ECAS, the identifier, the site and the time will be recorded in a log file. We do not record the time you spent logged in to a site. However, if you logout of ECAS, which is not normally necessary, the time at which you do so will be recorded.

Note: use of cookies

ECAS uses cookies to allow you to log in to different applications without re-entering your username and password. These cookies contain no personal information whatsoever, merely a pointer allowing the authentication service to find your entry in its own tables. The cookies are 'per-session' cookies, i.e. they are destroyed when you close your browser. If you have chosen the option for your browser not to accept such cookies, you will not benefit from this feature and will have to re-authenticate yourself each time you log in to a different client application of the authentication service.
A persistent cookie may be created for your convenience in order to record your choice of language, and at your discretion, your username. In the absence of this cookie, the default language is English.

3. Who has access to your information and to whom is it disclosed?

By registering yourself, you authorise the disclosure of the details you have entered in the user registration system to any Commission site that you access after having given your username and password. If you were registered by your organisation, your consent is assumed to have been given (implicitly or explicitly) for the transfer of your details.

The details of the activity associated with your account are never passed to any other Commission site by IMS.

The Commission will not divulge your information to third parties outside the Informatics DG with the following exceptions:

- the duly authorised support unit or help desk responsible for the domain in which you are registered
- duly authorised bodies, on a case by case basis: OLAF, internal Commission Security Directorate or disciplinary bodies, the Ombudsman, the EDPS.

To preserve your privacy, you can choose (through an option on the login screen) to be notified whenever a relying party (i.e. a Commission site) requests your identity - you will have the option to cancel the operation before any information is passed. However, this may render the application inaccessible to you. If, having logged in into ECAS, you wish to access sites anonymously, you can do one of the following before connecting to the site in question:

- open a new browser session and use it to access the site
- logout from the authentication service
- disable cookies in your browser options

Note that behaviour varies from browser to browser and may affect the results of these operations.

If you need to access a Commission site that requires you to register and authenticate, but you do not wish it to have access to the details you supplied in order to gain access to another Commission site, we suggest you create a separate account for this purpose. This will require you to provide a distinct e-mail address, which need not be traceable to you personally. Of course, this may deny you access to certain sites which require proof of identity.

Your password is stored only in an irreversible form. Apart from your password, the service administrators can view all of the data pertaining to a particular user. This helps them to perform duties such as helping users with problems and diagnosing suspected security incidents.

4. How do we protect and safeguard your information?

The Commission stores your personal information in secure computers and your information can only be accessed by authorised persons and internal sites.

When you login, the password is always encrypted on the network and is decrypted for checking against the stored password by the authentication service, not by the individual site. All passwords (including previous passwords mentioned above) are stored in a form that permits them to be checked against a supplied value, but their actual value cannot be derived from the stored value.

The details about your user account are available only to yourself and the service administrators.

If you registered yourself directly, you should be aware that anyone with access to read your e-mail may be able to use the account you create and acquire the identity it represents. You are responsible for assessing the risk that this presents to you personally.

Similarly, certain users are allowed to reset their password using e-mail. They should bear in mind that anyone else with access to their e-mail (because of automatic forwarding, delegation or other reasons) will be able to reset the password.

For this reason, in order to perform important business or access sensitive information, the Commission requires more stringent identity checks and your account will need to be set up or transformed specifically for this purpose. You will need to contact the relevant Commission department or a delegated representative in your organisation to achieve this.

If you have any reason to believe that your password has been compromised – for example, if your password appears to have been changed without your knowledge - you should notify your normal support contact or contact the Commission as described on the user registration and authentication pages.

Notes:

In principle, and especially if you have access to sensitive systems, you should never reveal your password to anybody else: it is a secret only you should know. In particular, your ECAS password should only ever be entered on screens showing the approved ECAS logo. Do not enter it if you have doubts about the authenticity of the ECAS site.

When you enter your password, make sure your browser indicates (usually by means of a padlock or other icon) that you are on a secure connection and that you are connected to a Commission site address (e.g. ec.europa.eu, webgate.eu-admin.net).

5. How can you verify, modify or delete your information?

You can verify your account information, including the data recorded about activity on your account, in the pages of either the user registration service or the Authentication Service (ECAS). This excludes information that is only held in log files: if you wish to access your log file entries, you may request it by writing to the Controller at the address given below. A response will be given within a period of six weeks from the date of receipt of the request.

In case of difficulty, you can obtain help by following the contact link below (see point 7).

If you registered yourself in the Commission's system, you will be able to change or remove any personal information on-line. However, if your details were registered through a third party, this may not be possible and you will have to contact that third party in order to have the information changed: you may nevertheless have the information removed by the Commission, but if the third party re-submits this information to the Commission, it will be re-instated.

Since it is collected automatically, it is not possible to modify any of the technical data held by the authentication service, with the exception of the password itself.

6. How long do we keep your data?

The Identity Management Service keeps your data for as long as you are recorded as an active user and for a period of one year thereafter. Data concerning users automatically registered from internal sources (in the Commission and certain other EU bodies) may be kept for as long as it is retained in the source system. If you were registered through a third party, the period of activity will usually correspond to a contractual link with that party or be subject to an expiration date. In other cases, the Commission will consider you active as long as you continue to use your account or until your account expires.

Note that in the case of users who registered with IMS themselves, the period of one year is extended in order to allow the exchange of e-mail with a user. This exchange will provide for the user to request an extension, thus resetting to zero the recorded period of inactivity. In the absence of a response from the user, all personal data will be erased.

Data from the Identity Management Service is backed up regularly by the Commission to ensure a correct system restore if necessary to restart operations. Furthermore, the Identity Management Service is closely monitored and all sensitive actions on the system are logged, including each authentication request. These logs (log files) are rotated regularly and removed from the active system after a maximum of six months in accordance with REGULATION (EC) No 45/2001. All log files backed up by the standard Commission's backup procedure will not be removed from back-up tapes until those tapes are recycled, but that log data will not be restored if system restore is required.

7. Contact Information

If you wish to ask questions or post complaints about the service with respect to the use of your personal information, you should follow the contact link that is shown on each Identity Management service page or write to the following address:

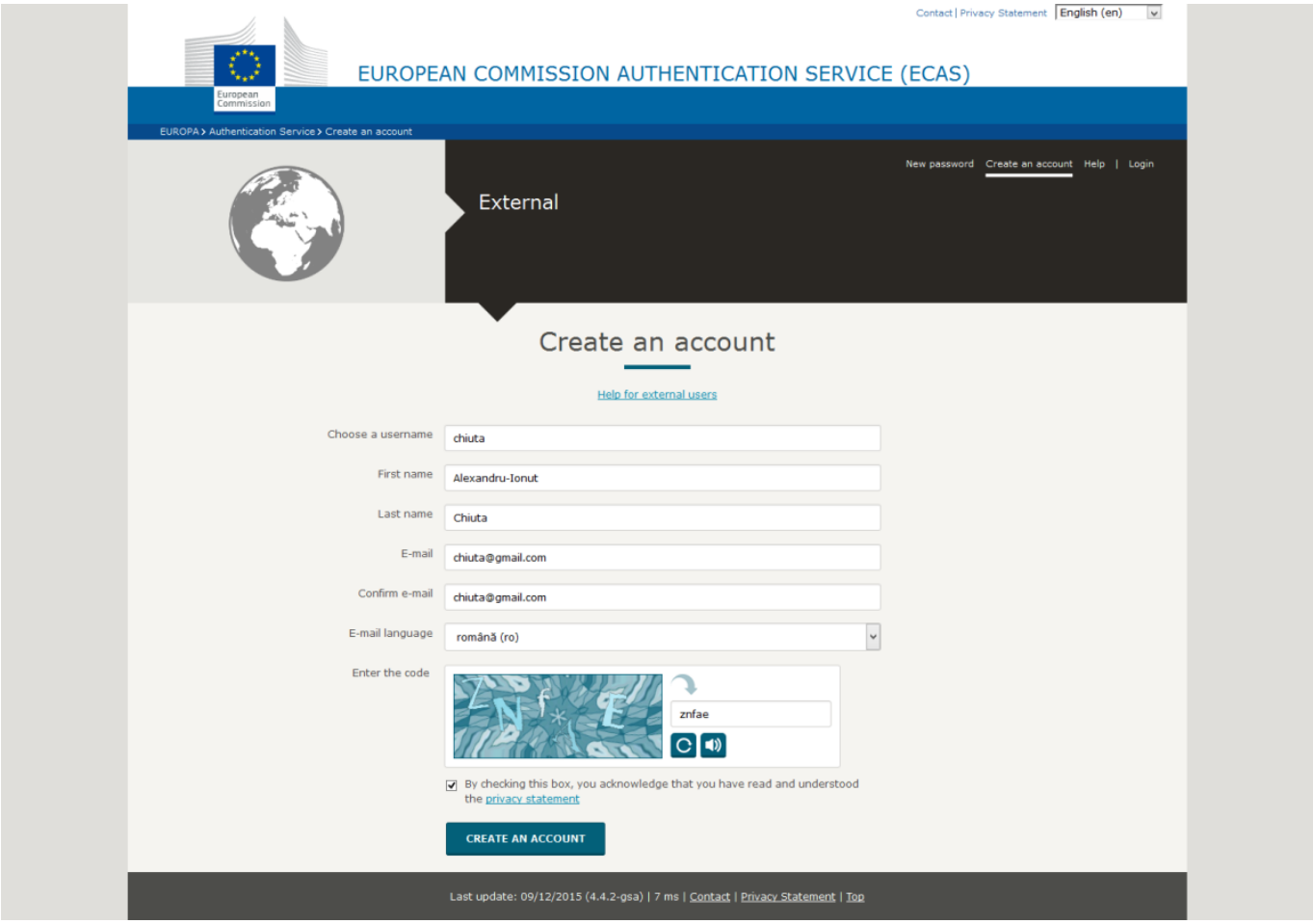
> The Director General
> Informatics DG
> European Commission
> 200 rue de la Loi
> B-1040 Brussels

8. Recourse

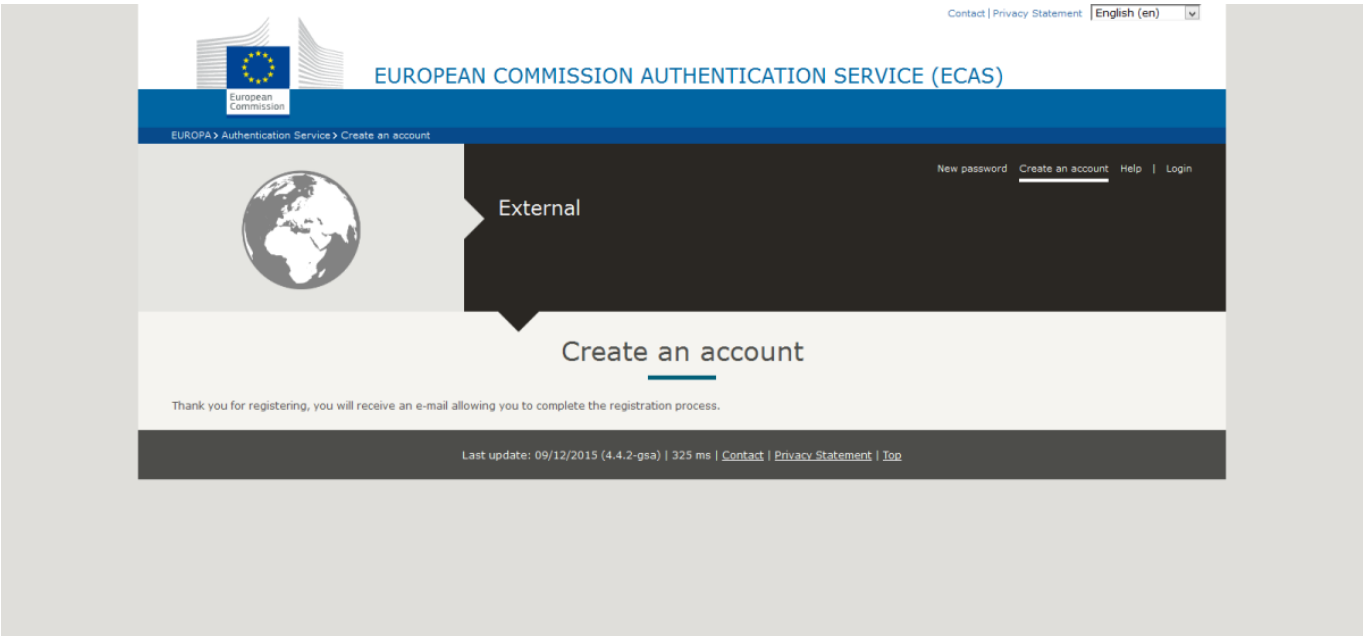
If necessary, complaints can be addressed to the European Data Protection Supervisor.

Last update: 09/12/2015 (4.4.2-gsa) | 2 ms | Top

2.5 regprof register date personale

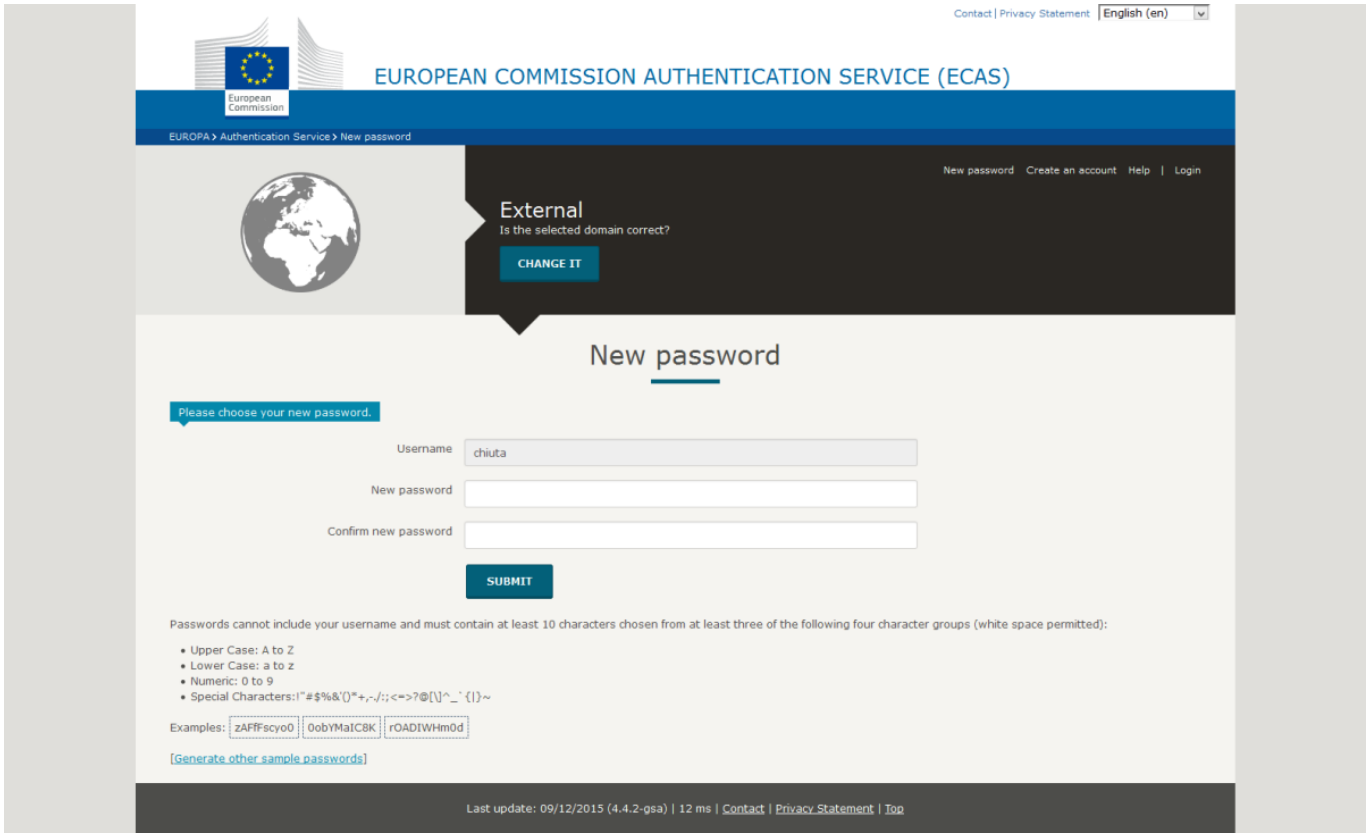


2.6 regprof register thank you for registering you will receive an e-mail allowing you to complete the registration process

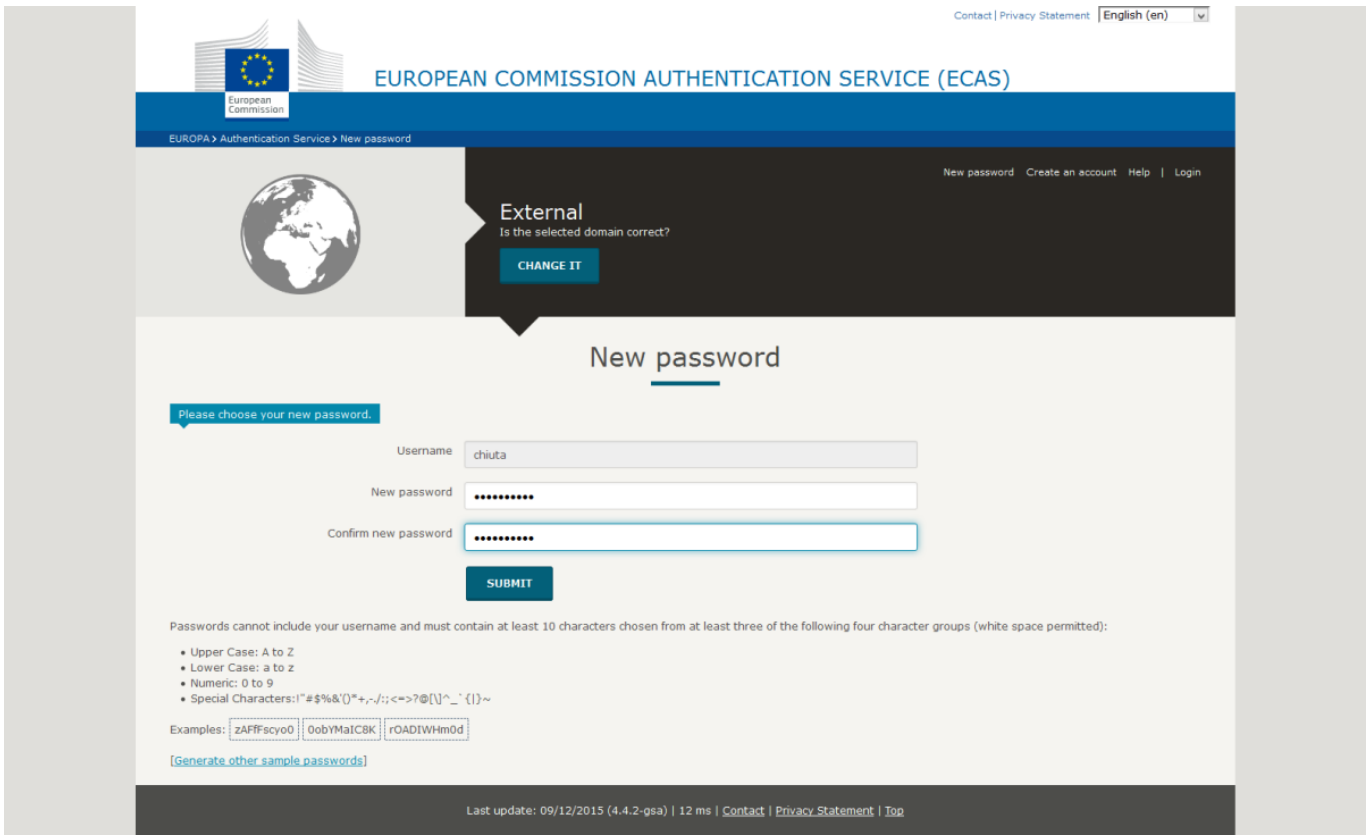


2.7 gmail parola dumneavoastră ECAS

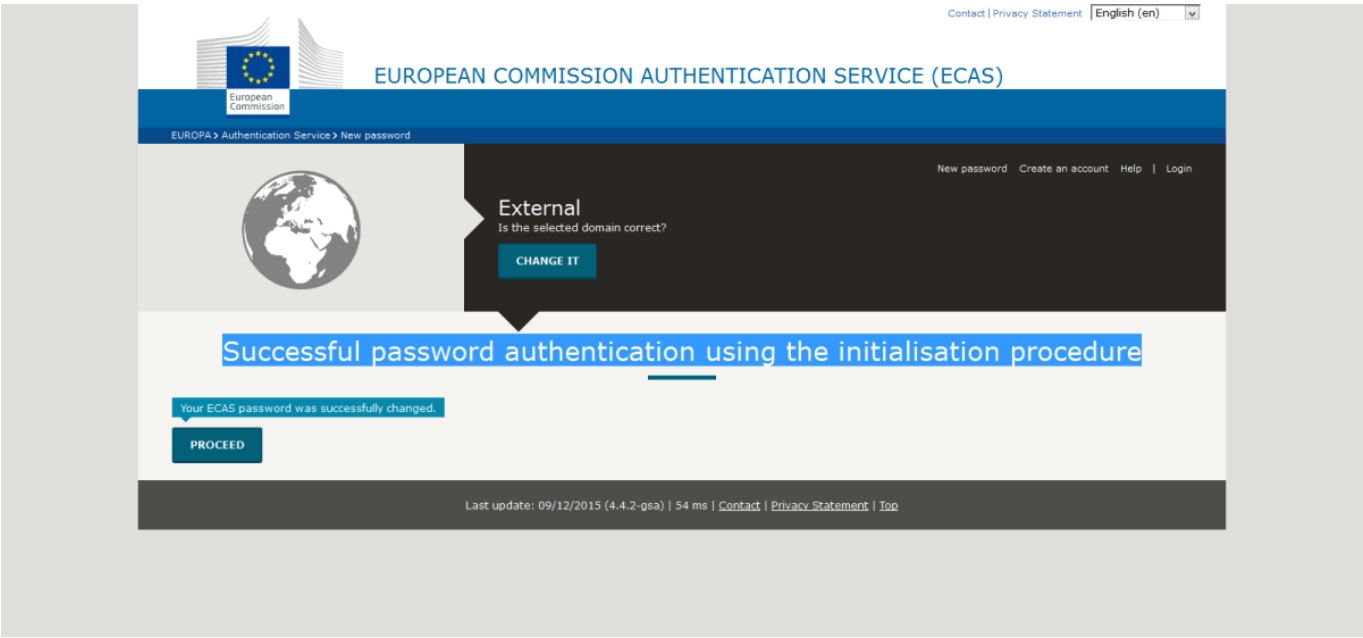
2.8 regprof register new password



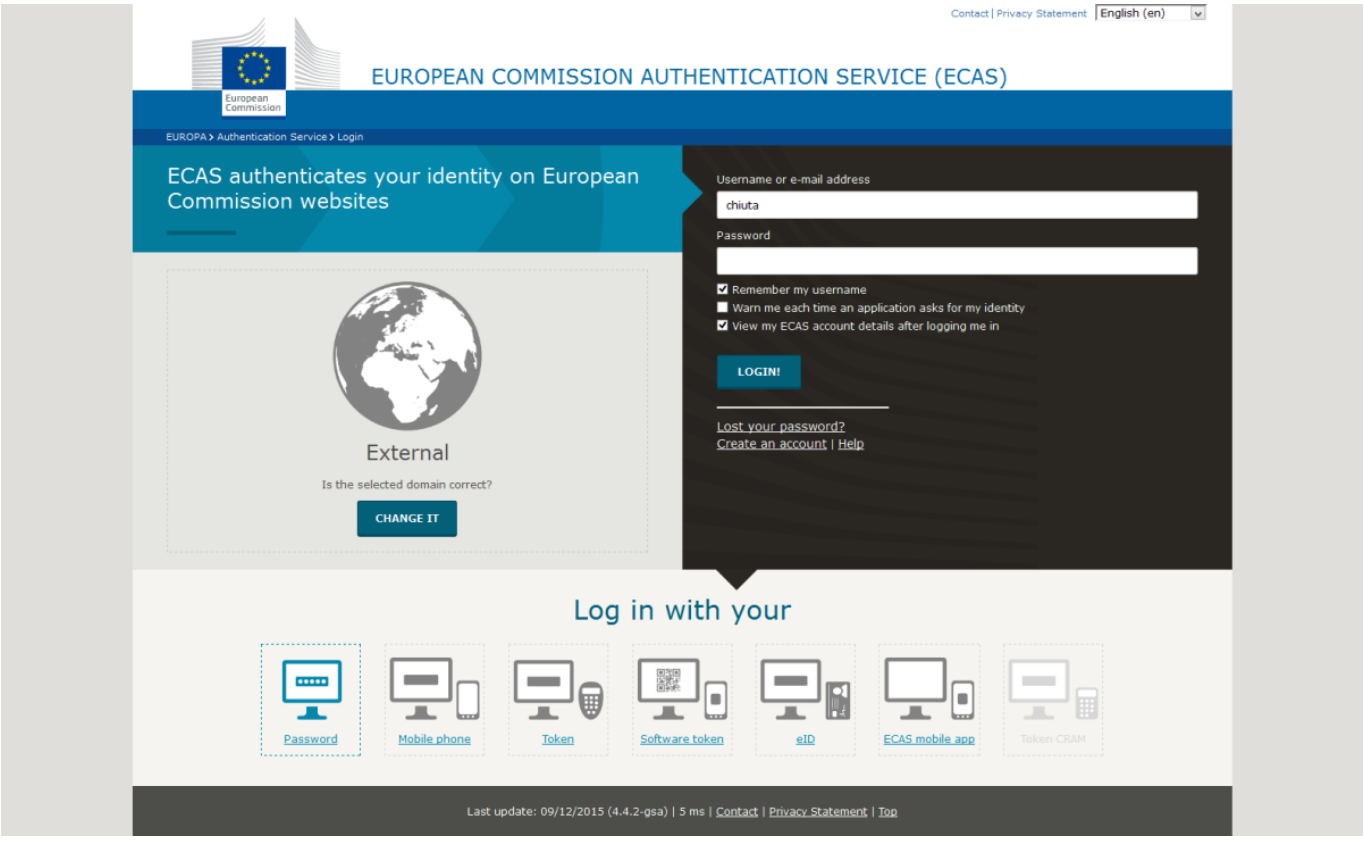
2.8,1 regprof register noua parola de minimum 10 caractere completata



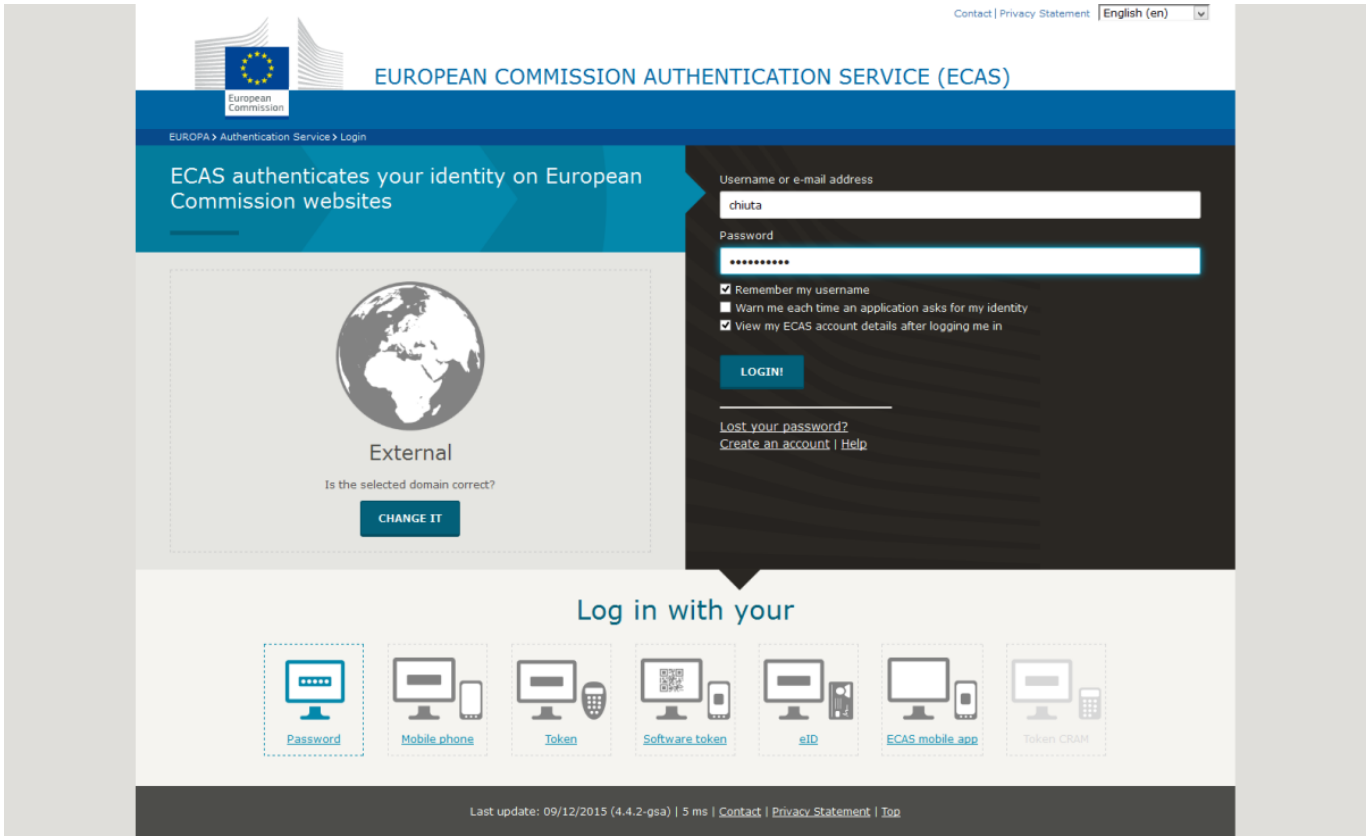
2.9 regprof register successful password authentication using the initialisation procedure



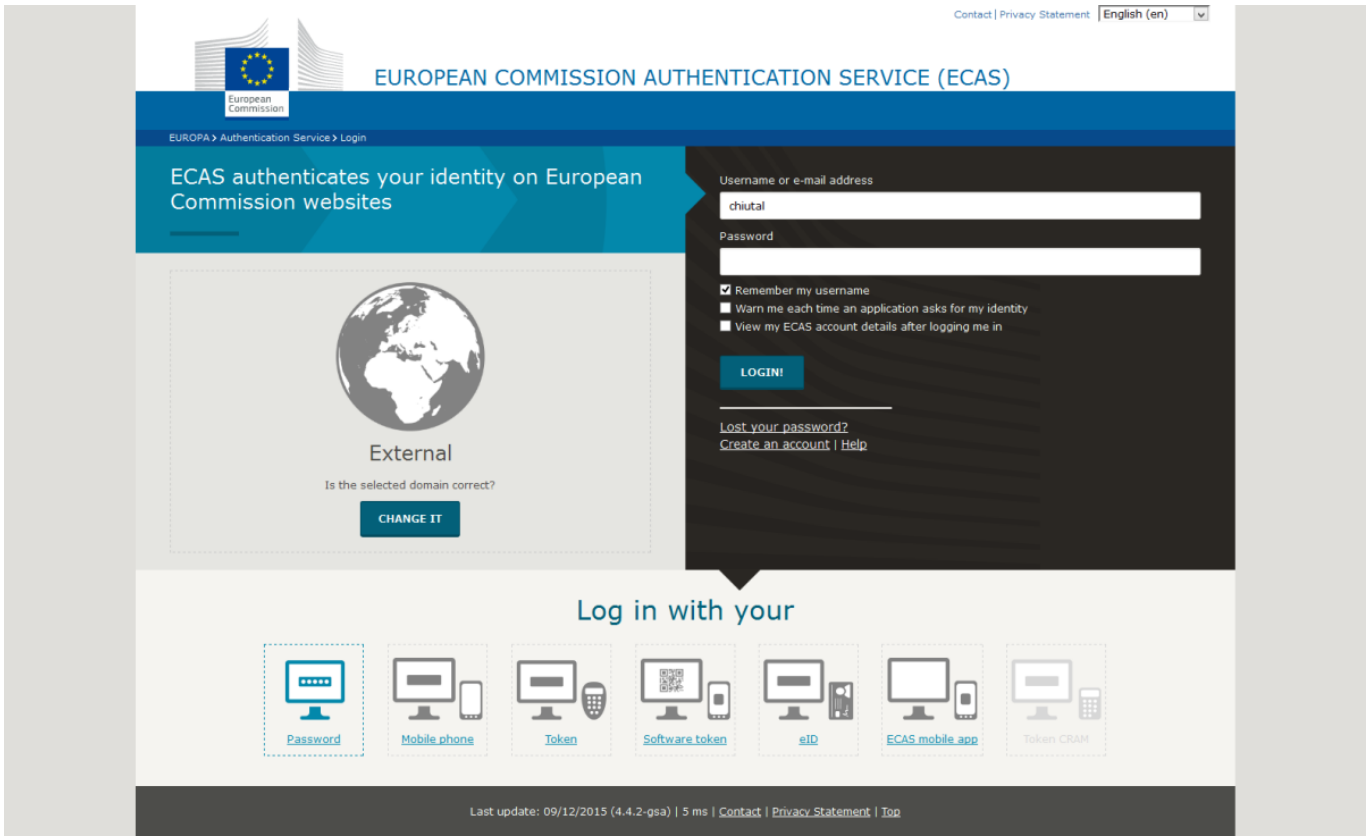
3.0 login external



3.0.1 external username password

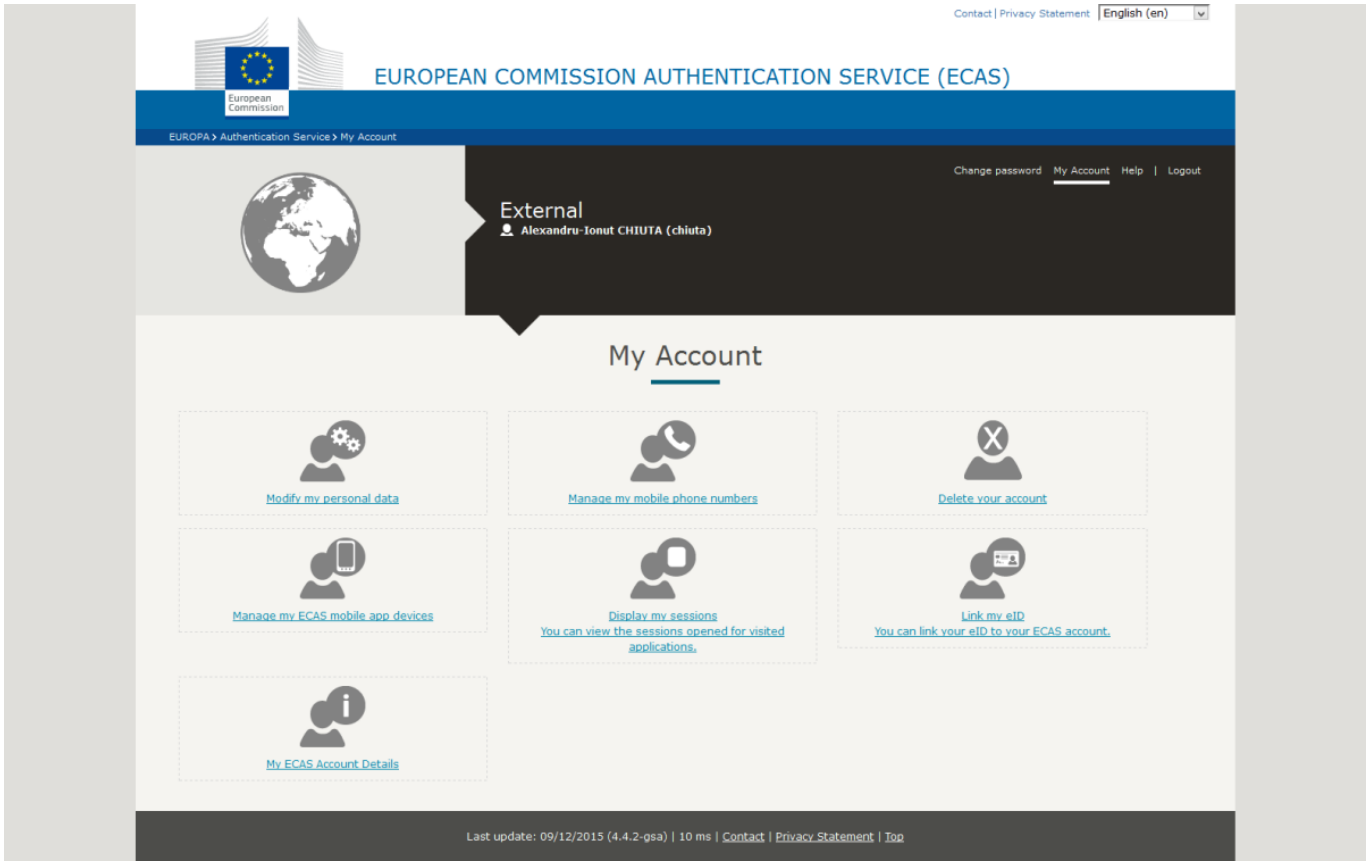


3.0.2 external username or e-mail address password remember my username

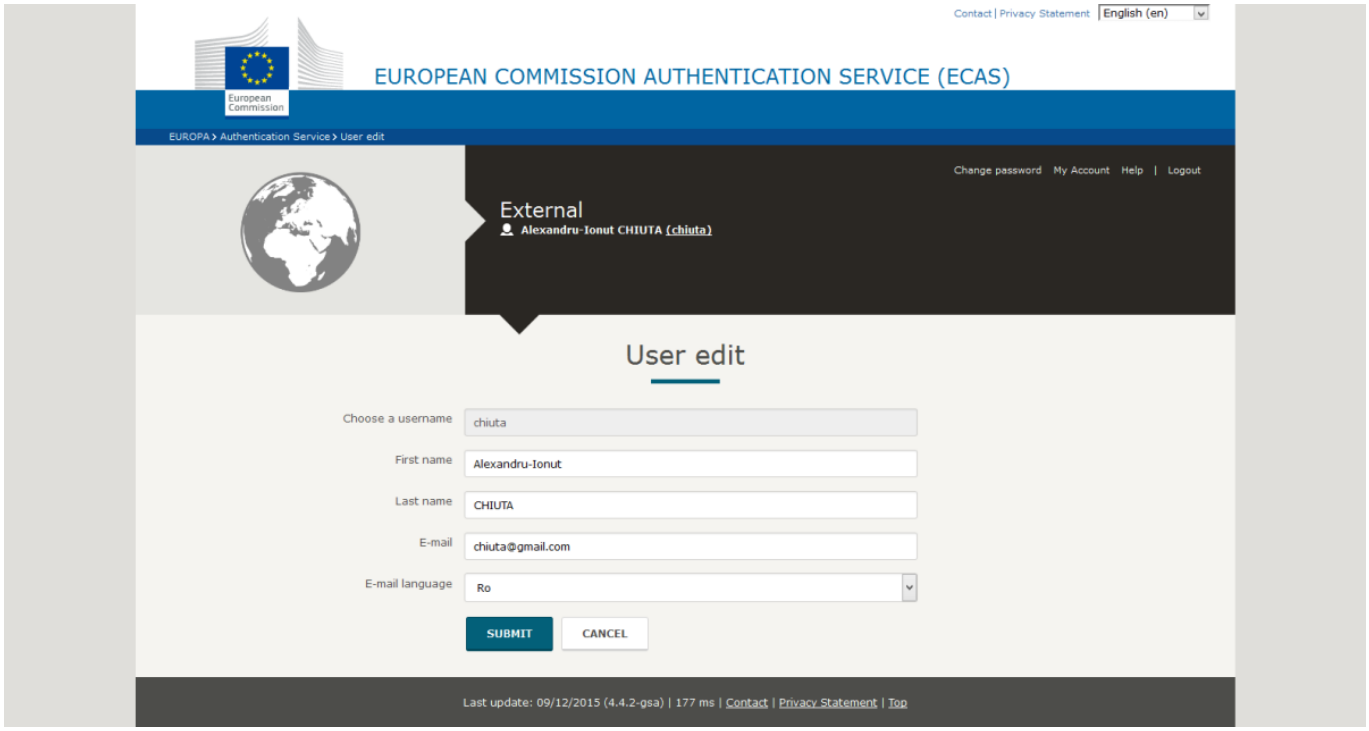


3.1 successful login my ecas account details

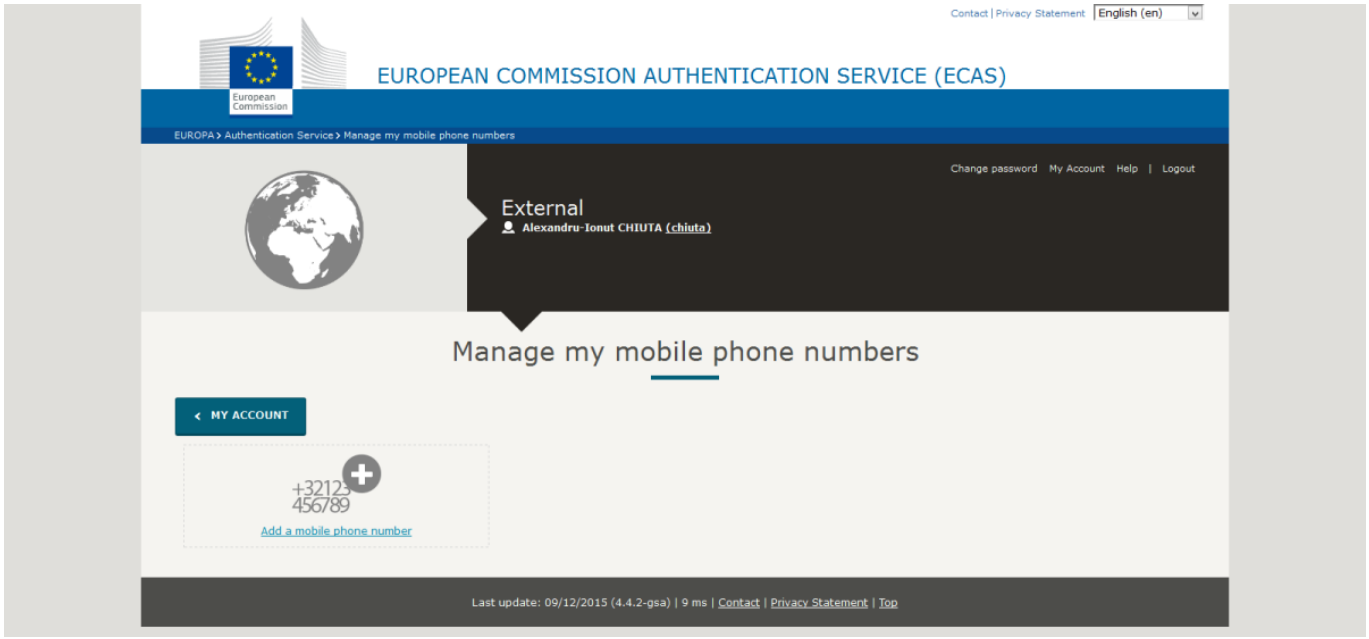
3.2 my account



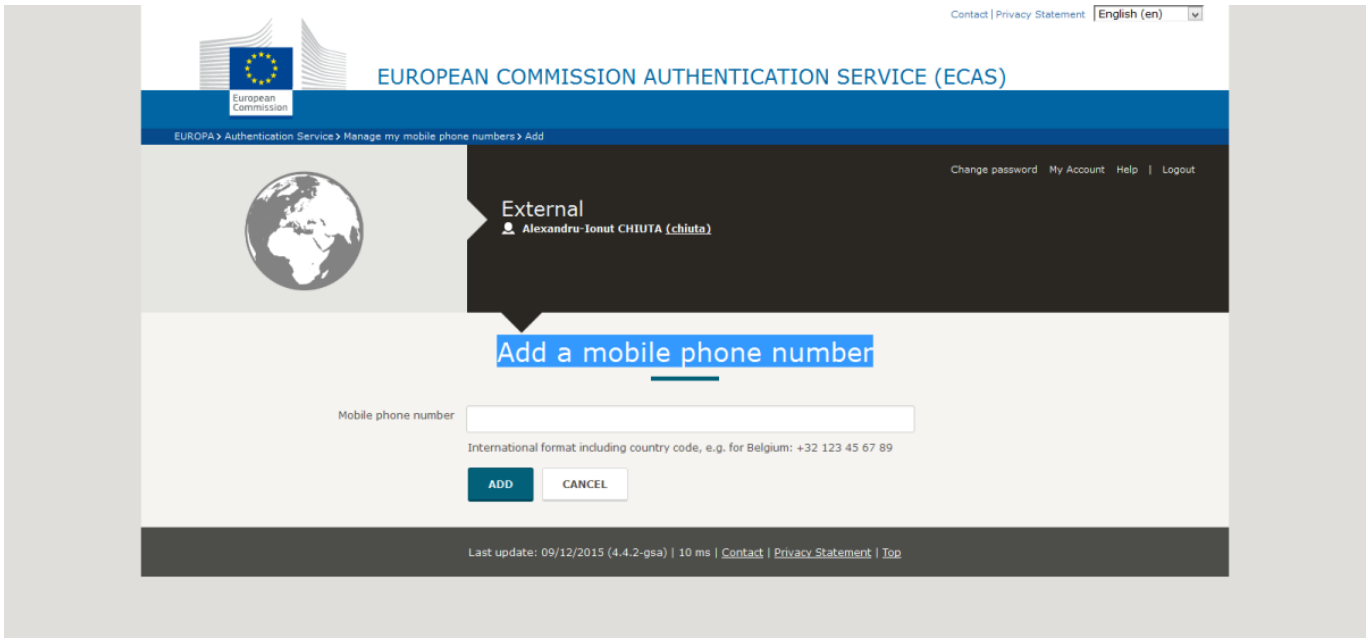
3.2.1 my account user edit



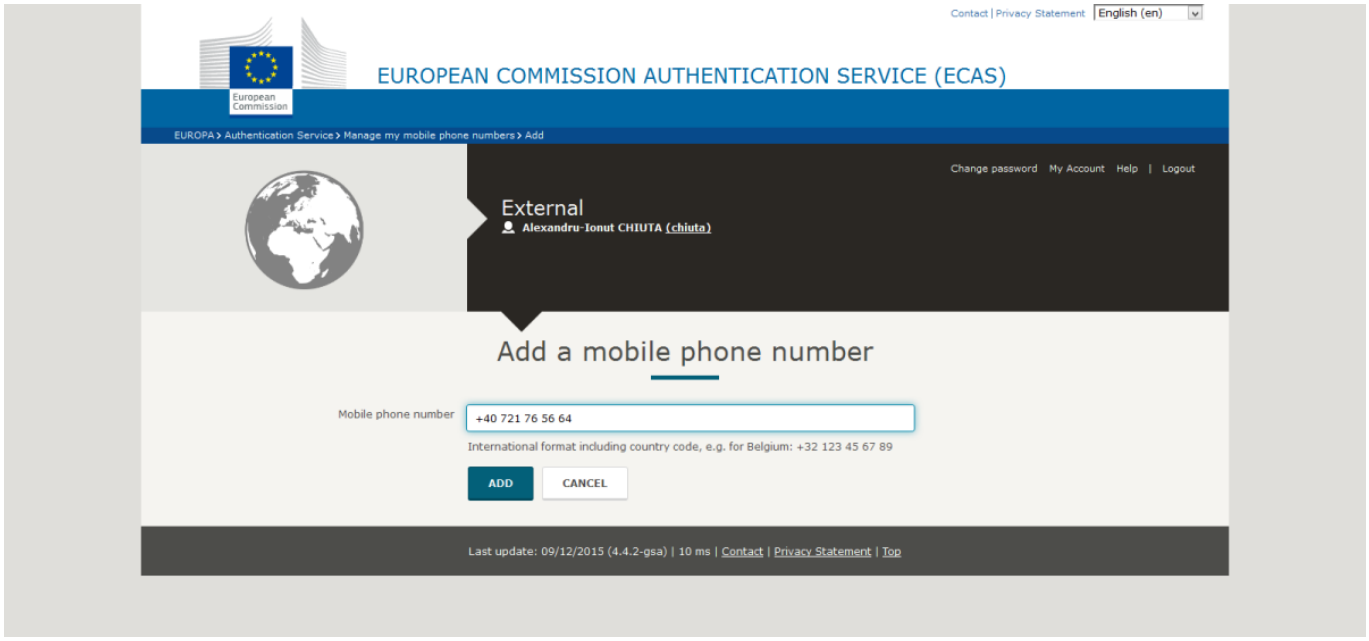
3.2.2 my account manage my mobile phone numbers



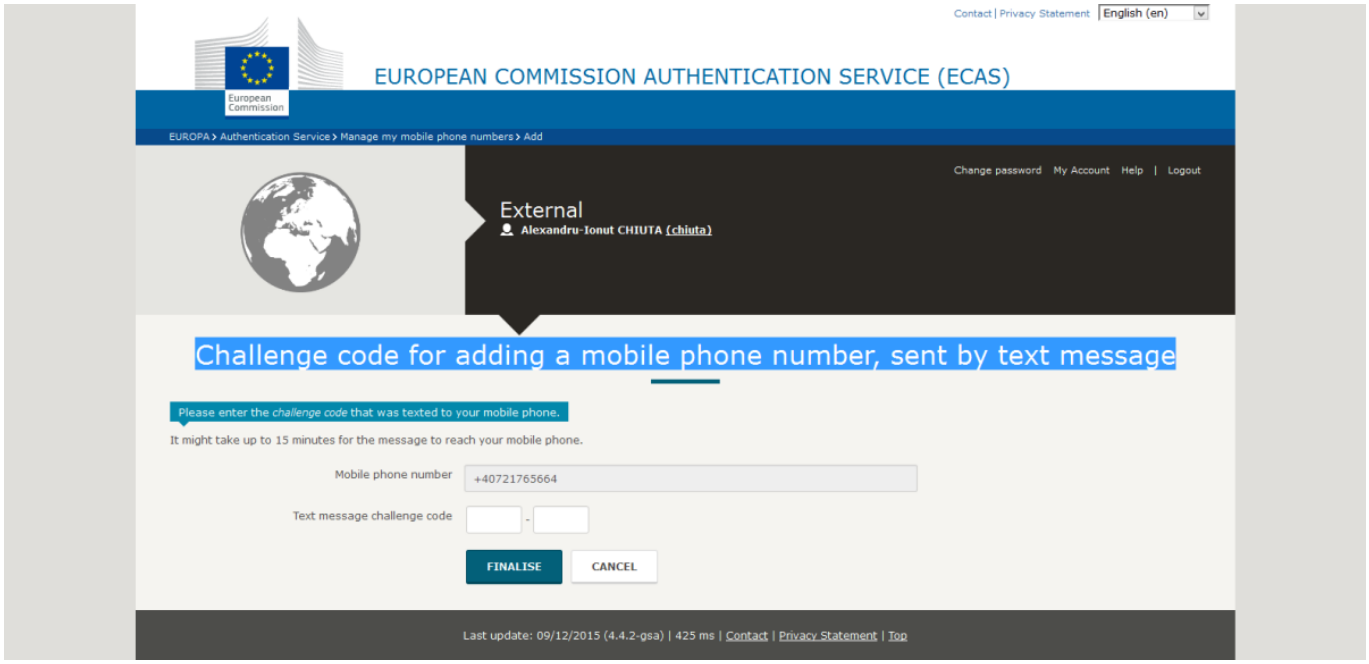
3.2.2.1 my account add a mobile phone number



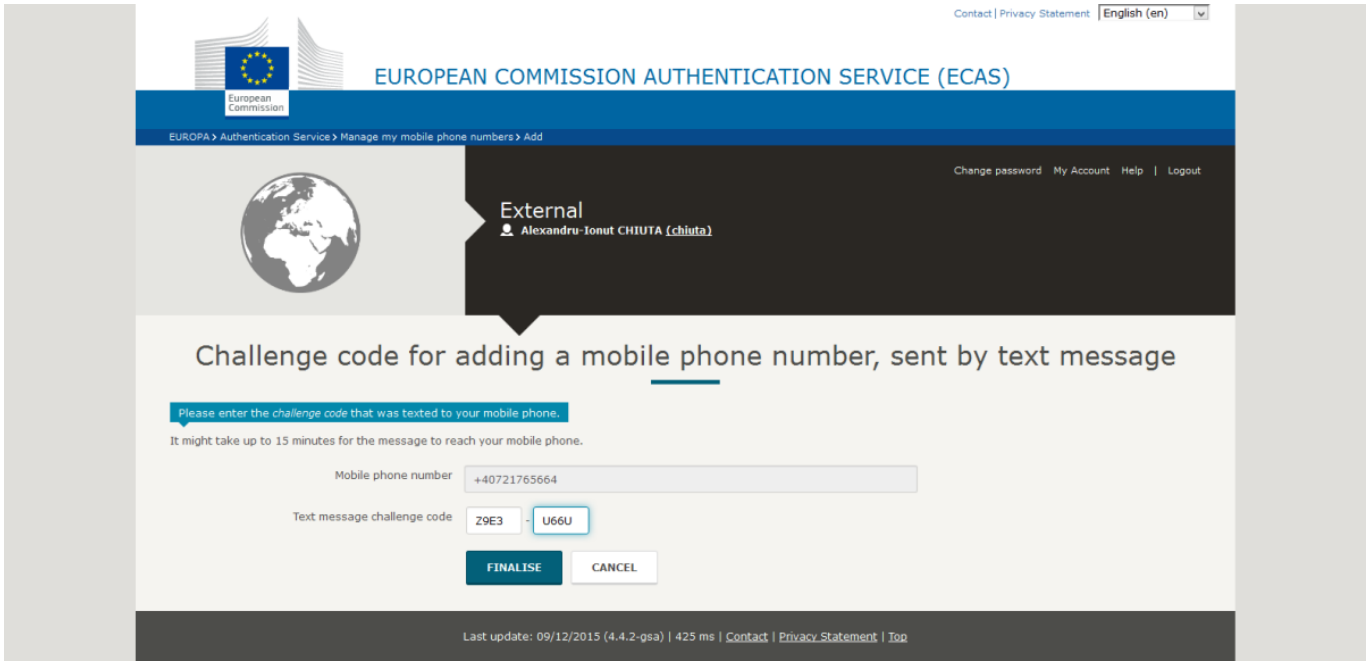
3.2.2.1.0 my account add a mobile phone number romanian mobile entered



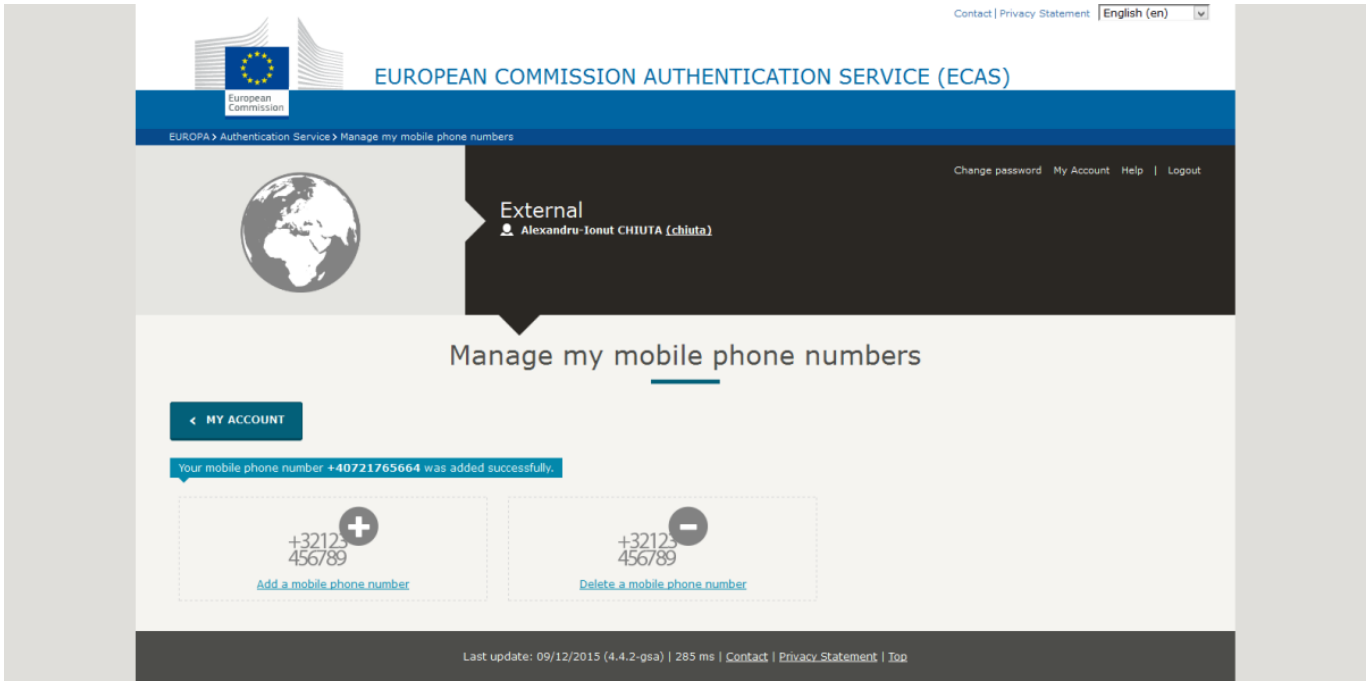
3.2.2.2 challenge code for adding a mobile phone number sent by text message



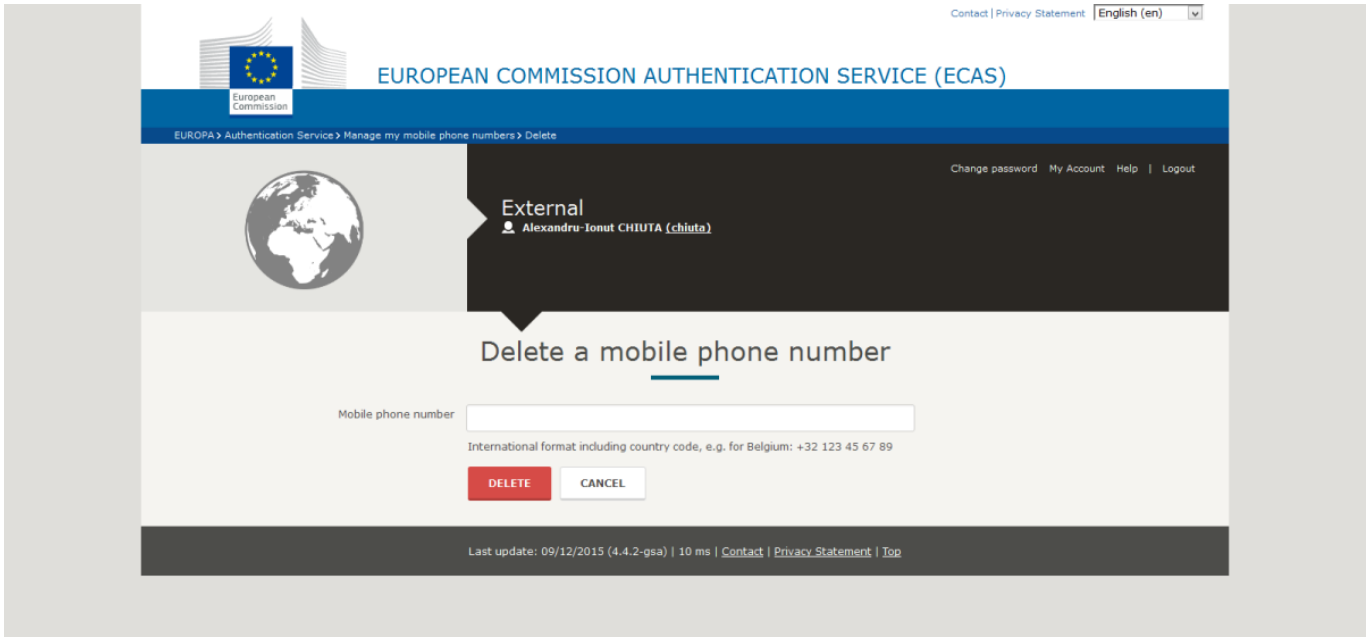
3.2.2.2.0 challenge code for adding a mobile phone number sent by text message text message challenge code entered



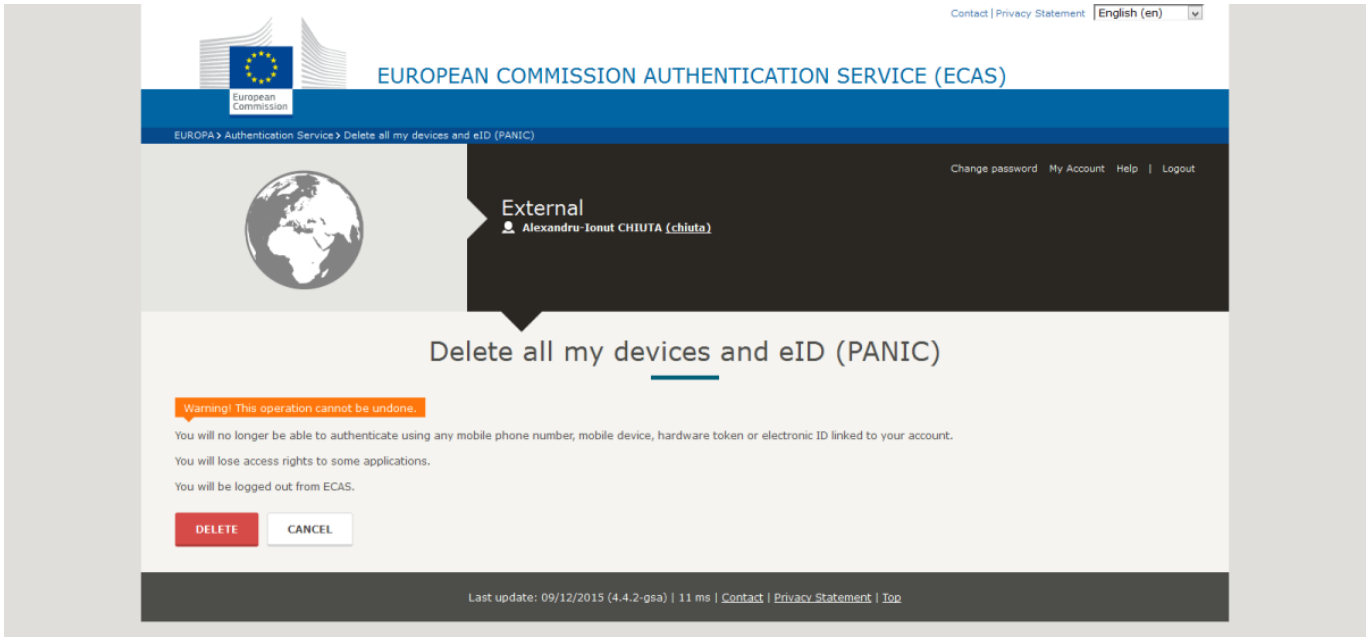
3.2.2.3 your mobile phone number was added successfully



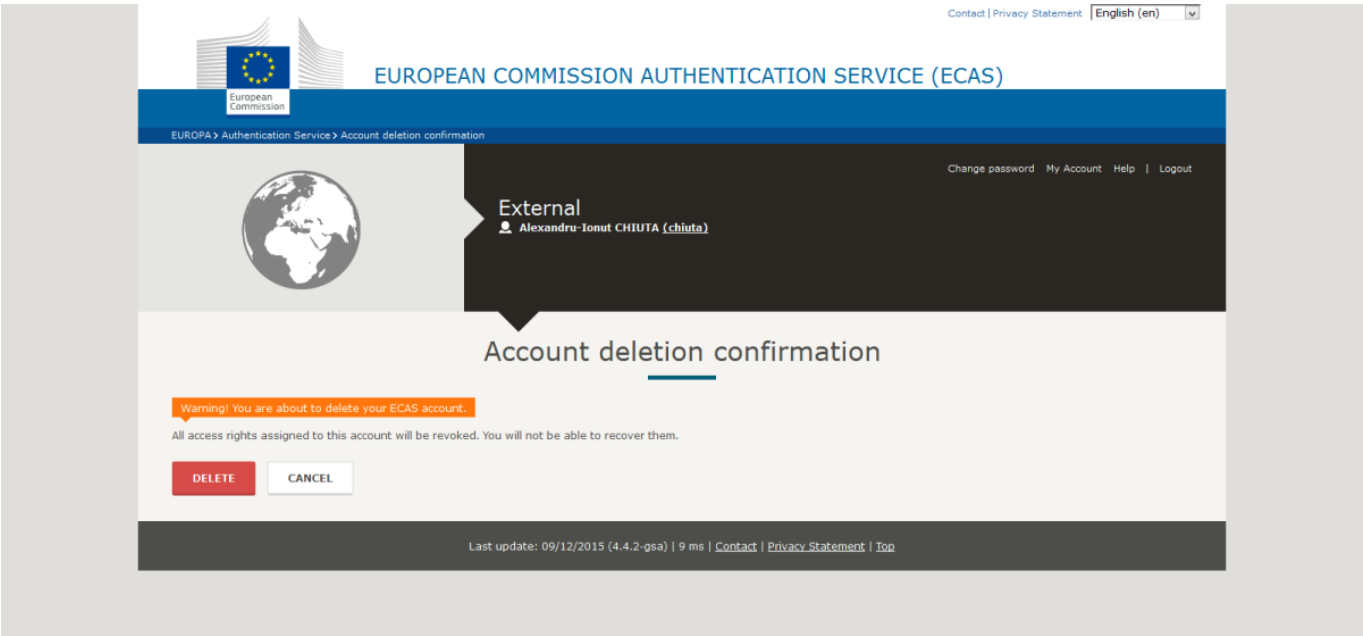
3.2.2.4 delete a mobile phone number



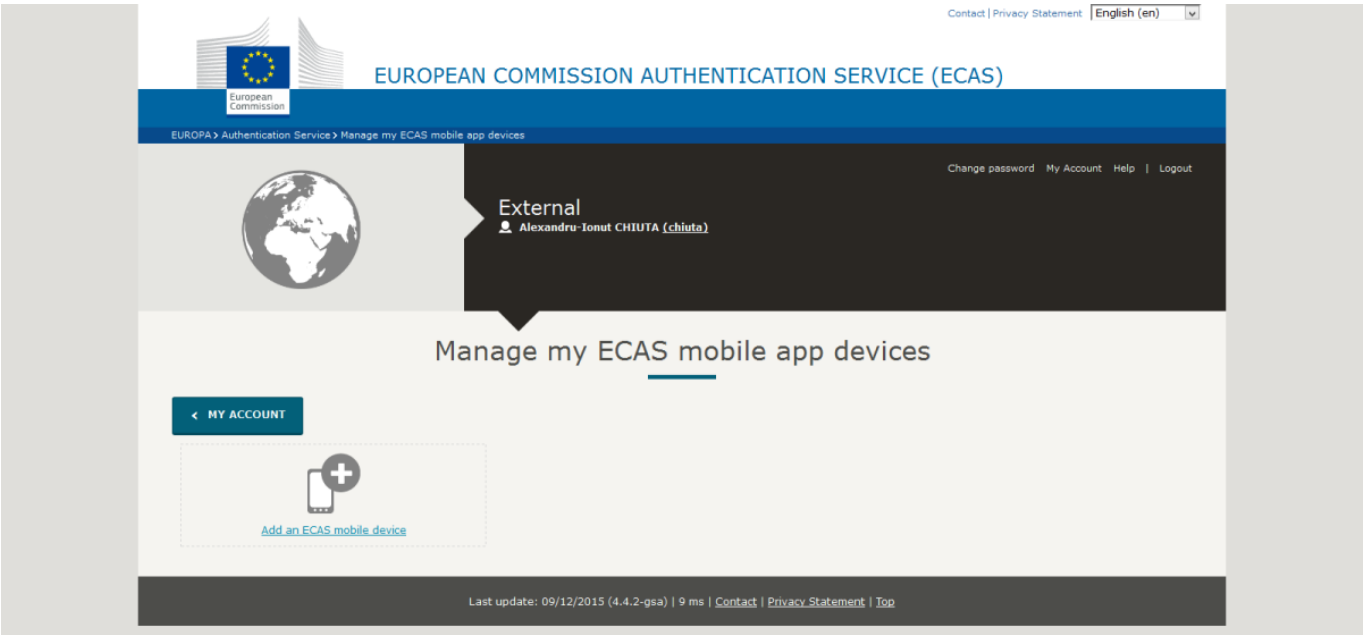
3.2.3 my account delete all my devices and eid panic



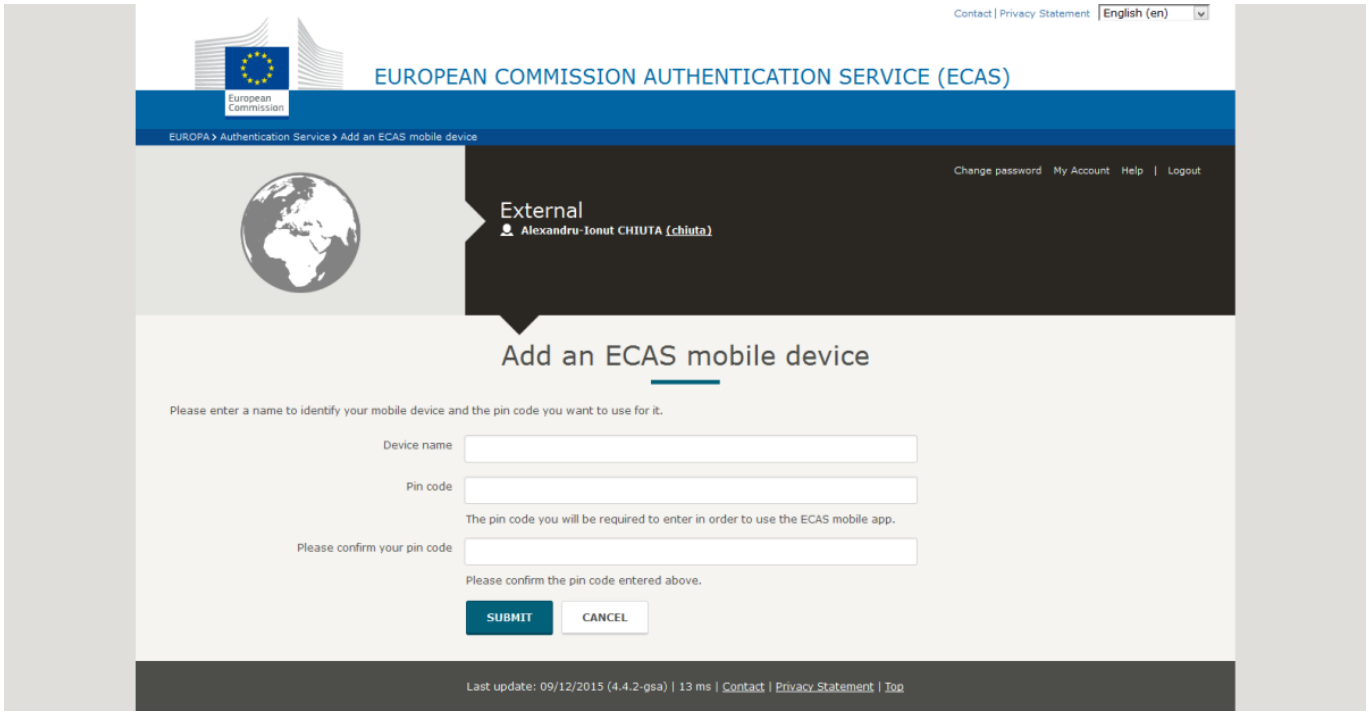
3.2.4 my account account deletion confirmation



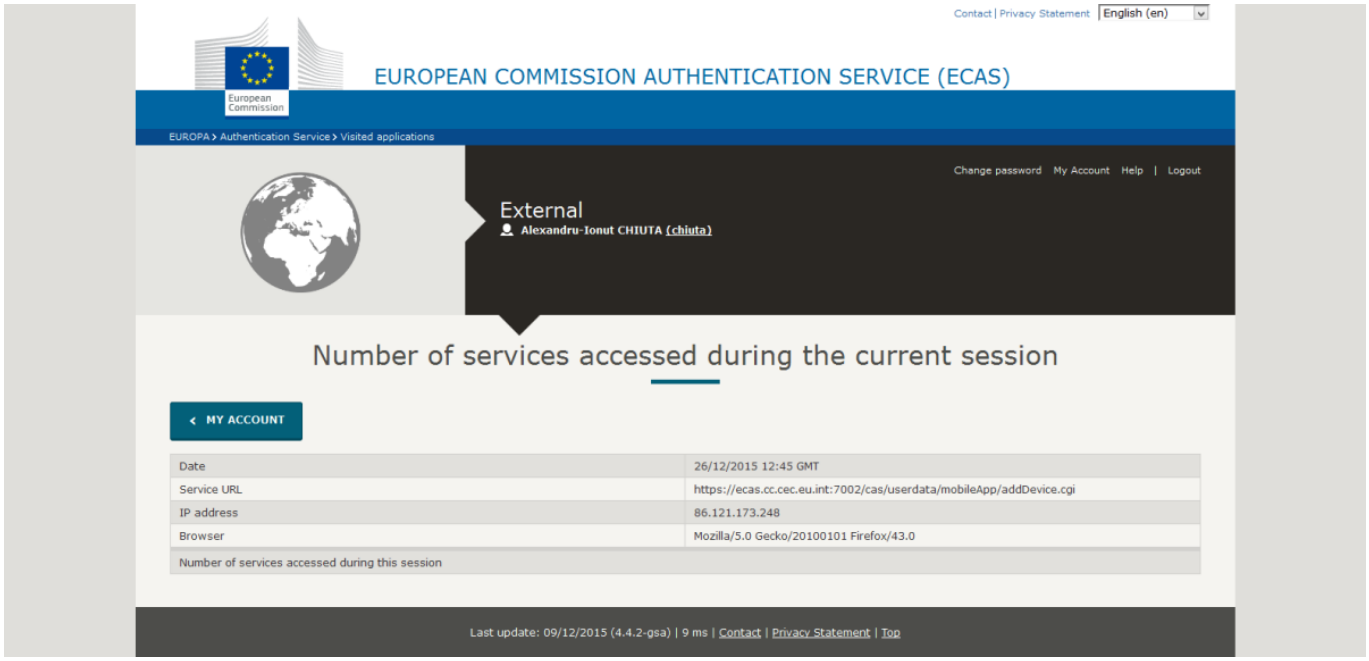
3.2.5 my account manage my ecas mobile app devices



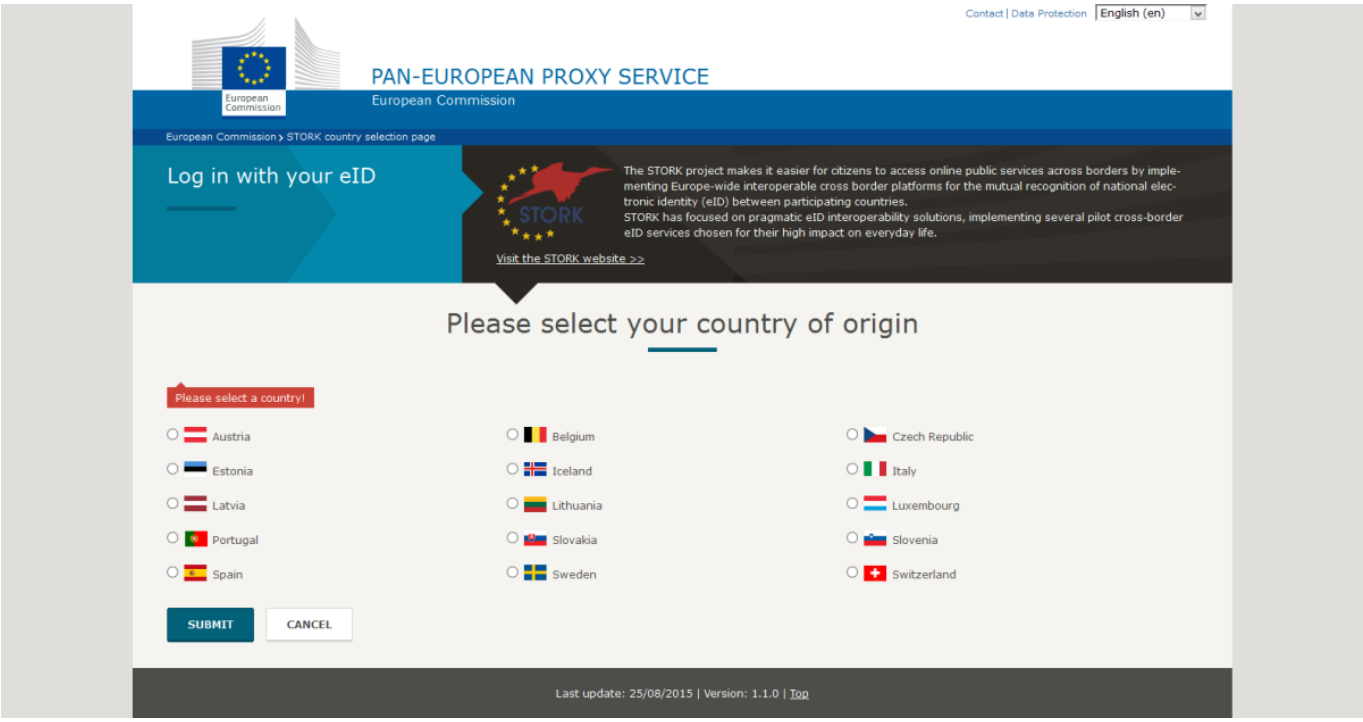
3.2.5.1 my account manage my ecas mobile app devices add an ecas mobile device



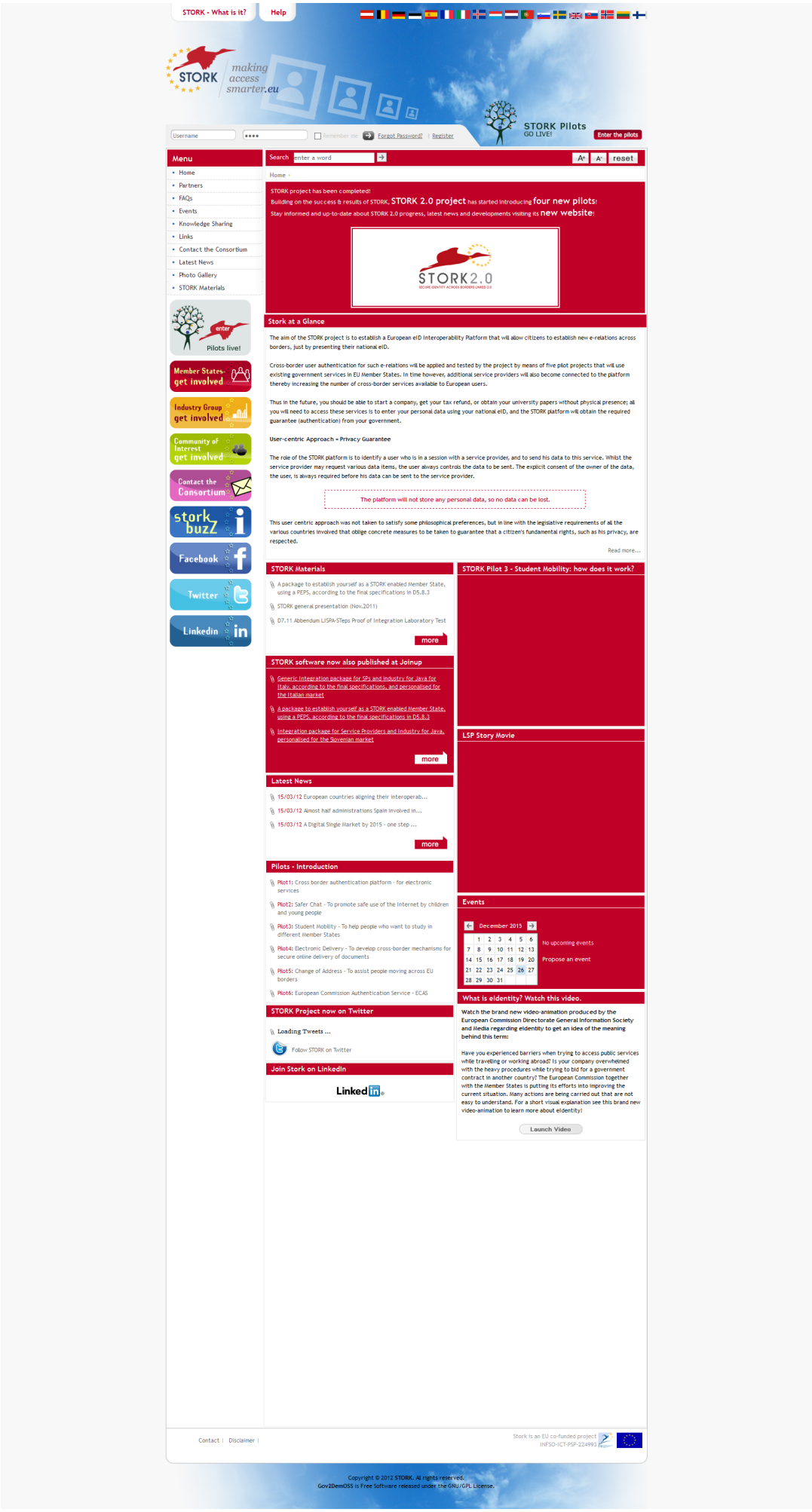
3.2.6 my account number of services accessed using the current session



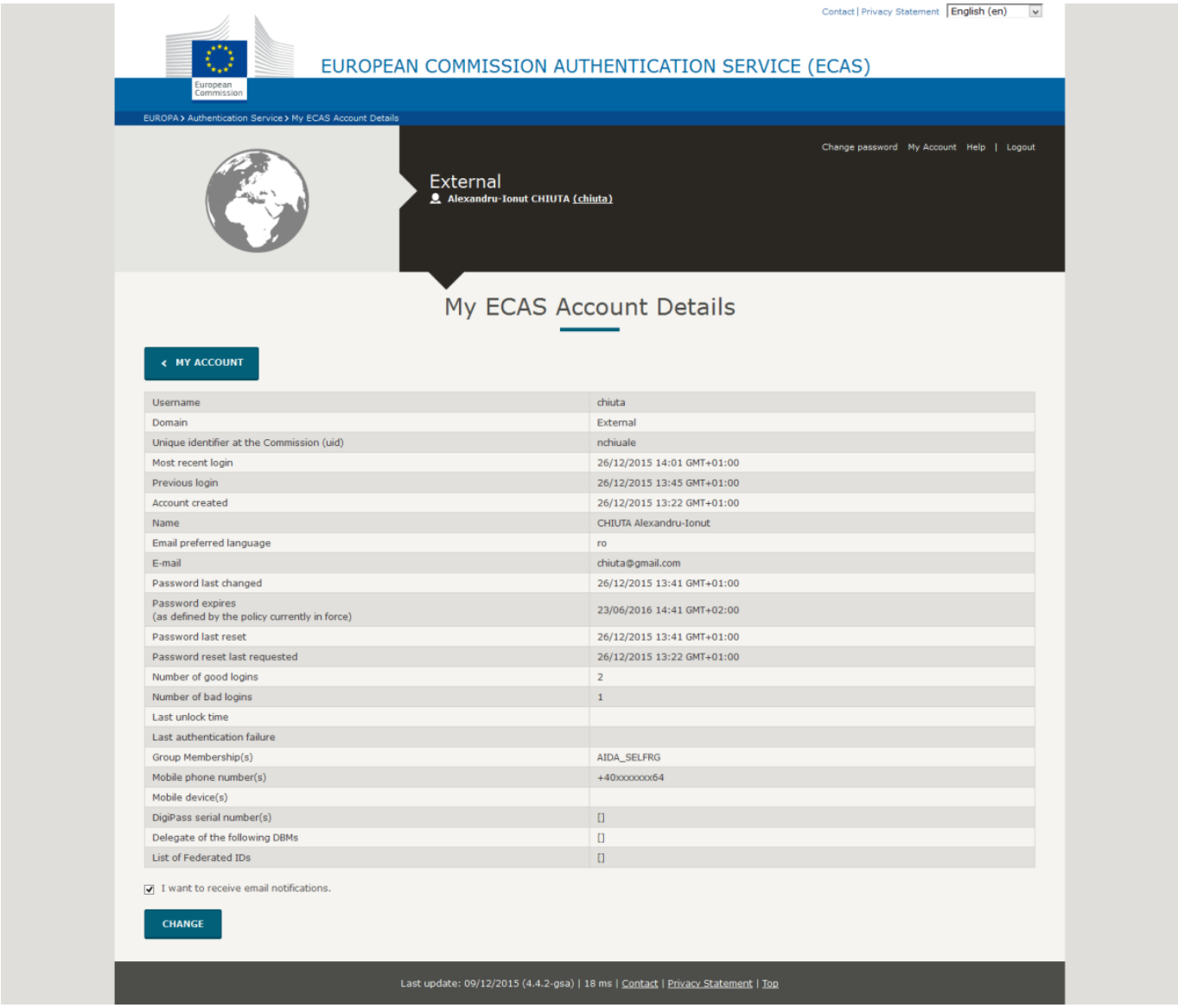
3.2.7 log in with your eid stork country selection page



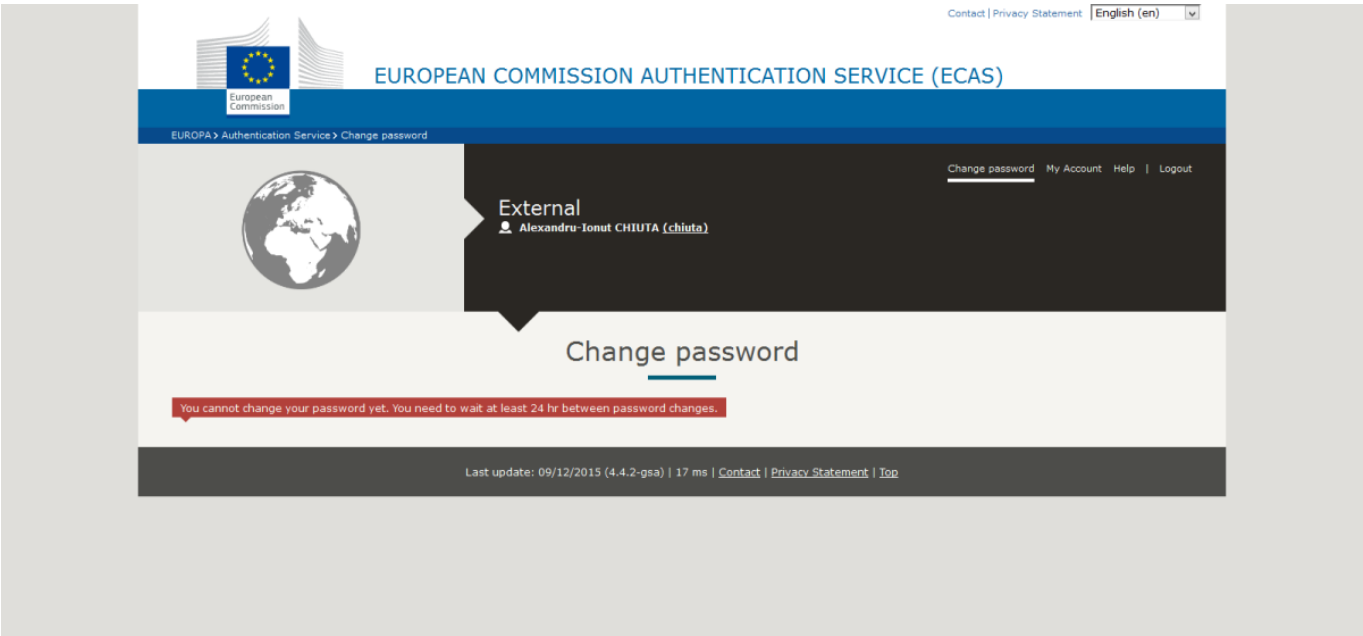
3.2.7.1 stork 2 website


STORK - What is it?
Help
STORK making access smarter.eu
STORK Pilots GO LIVE!
Enter the pilots
Username
Forgot Password?
Register
Menu
Home
Partners
FAQs
Events
Knowledge Sharing
Links
Contact the Consortium
Latest News
Photo Gallery
STORK Materials
Search
enter a word
reset
Home
STORK project has been completed!
Building on the success & results of STORK, STORK 2.0 project has started introducing four new pilots!
Stay informed and up-to-date about STORK 2.0 progress, latest news and developments visiting its new website!
STORK2.0
Stork at a Glance
The aim of the STORK project is to establish a European eID Interoperability Platform that will allow citizens to establish new e-relations across borders, just by presenting their national eID.
Cross-border user authentication for such e-relations will be applied and tested by the project by means of five pilot projects that will use existing government services in EU Member States. In time however, additional service providers will also become connected to the platform thereby increasing the number of cross-border services available to European users.
Thus in the future, you should be able to start a company, get your tax refund, or obtain your university papers without physical presence; all you will need to access these services is to enter your personal data using your national eID, and the STORK platform will obtain the required guarantee (authentication) from your government.
User-centric Approach = Privacy Guarantee
The role of the STORK platform is to identify a user who is in a session with a service provider, and to send his data to this service. Whilst the service provider may request various data items, the user always controls the data to be sent. The explicit consent of the owner of the data, the user, is always required before his data can be sent to the service provider.
The platform will not store any personal data, so no data can be lost.
This user centric approach was not taken to satisfy some philosophical preferences, but in line with the legislative requirements of all the various countries involved that oblige concrete measures to be taken to guarantee that a citizen's fundamental rights, such as his privacy, are respected.
Read more...
Pilots live!
Member States get involved
Industry Group get involved
Community of Interest get involved
Contact the Consortium
stork buzz
Facebook
Twitter
Linkedin
STORK Materials
A package to establish yourself as a STORK enabled Member State, using a PEPS, according to the final specifications in D5.8.3
STORK general presentation (Nov.2011)
D7.11 Abbendum LISPA-STeps Proof of Integration Laboratory Test
more
STORK software now also published at Joinup
Generic Integration package for SPs and industry for Java for Italy, according to the final specifications, and personalised for the Italian market
A package to establish yourself as a STORK enabled Member State, using a PEPS, according to the final specifications in D5.8.3
Integration package for Service Providers and industry for Java, personalised for the Slovenian market
more
Latest News
15/03/12 European countries aligning their interoperab...
15/03/12 Almost half administrations Spain involved in...
15/03/12 A Digital Single Market by 2015 - one step ...
more
Pilots - Introduction
Pilot1: Cross border authentication platform - for electronic services
Pilot2: Safer Chat - To promote safe use of the Internet by children and young people
Pilot3: Student Mobility - To help people who want to study in different Member States
Pilot4: Electronic Delivery - To develop cross-border mechanisms for secure online delivery of documents
Pilot5: Change of Address - To assist people moving across EU borders
Pilot6: European Commission Authentication Service - ECAS
STORK Project now on Twitter
Loading Tweets ...
Follow STORK on Twitter
Join Stork on LinkedIn
LinkedIn
STORK Pilot 3 - Student Mobility: how does it work?
LSP Story Movie
Events
December 2015
No upcoming events
Propose an event
What is eIdentity? Watch this video.
Watch the brand new video-animation produced by the European Commission Directorate General Information Society and Media regarding eIdentity to get an idea of the meaning behind this term:
Have you experienced barriers when trying to access public services while travelling or working abroad? Is your company overwhelmed with the heavy procedures while trying to bid for a government contract in another country? The European Commission together with the Member States is putting its efforts into improving the current situation. Many actions are being carried out that are not easy to understand. For a short visual explanation see this brand new video-animation to learn more about eIdentity!
Launch Video
Contact | Disclaimer |
Stork is an EU co-funded project INFSO-ICT-PSP-224993
Copyright © 2012 STORK. All rights reserved.
Gov2DemOSS is Free Software released under the GNU/GPL License.

3.2.8 my ecas account details



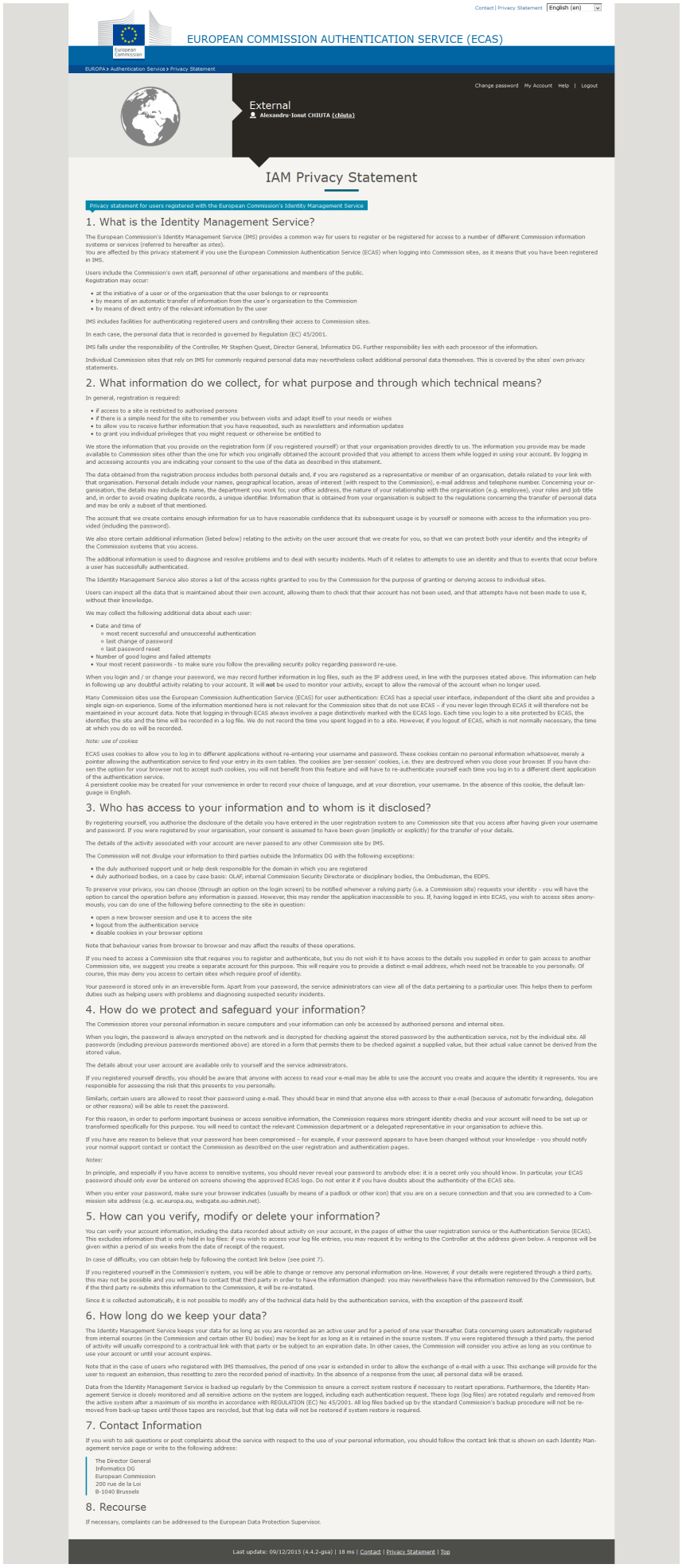
3.3 change password


Contact | Privacy Statement
English (en)
EUROPEAN COMMISSION AUTHENTICATION SERVICE (ECAS)
European Commission
EUROPA > Authentication Service > Change password
Change password
My Account
Help
Logout
External
Alexandru-Ionut CHIUTA (chiuta)
Change password
You cannot change your password yet. You need to wait at least 24 hr between password changes.
Last update: 09/12/2015 (4.4.2-gsa) | 17 ms | Contact | Privacy Statement | Top

3.4 contact

Contact | Privacy Statement
English (en)
EUROPEAN COMMISSION AUTHENTICATION SERVICE (ECAS)
European Commission
EUROPA > Authentication Service > Contact
Change password
My Account
Help
Logout
External
Alexandru-Ionut CHIUTA (chiuta)
Contact
ECAS, the European Commission Authentication Service, enables you to access various Web applications centrally, using the same username and password.
ECAS is a separate entity from the applications it protects. Once you have logged in, what happens depends on the application protected by ECAS, not on ECAS itself.
External users
If your username was assigned by a Commission service provider or another contact/support team at the Commission, please contact them in the first instance.
The sites in question should provide contact information on pages for which you do not have to login.
• If you are an external user having difficulties in registering yourself for access to Commission systems
• and you have tried the suggestions provided through the Help links on the login page, but this has not solved your problem
• and you are sure your problem has something to do with your registration or your username/password in ECAS, not with the application protected by ECAS
To help us help you as efficiently as possible:
1. Please gather the following information:
• the username or e-mail address of the account(s) concerned
• the nature of your relationship with the Commission (short-term contract, permanent contract, seconded national expert, service provider?)
• the application concerned
• how you are accessing this application (including its URL, which should be different from the ECAS URL)
• the source of the URL you are using (e-mail, link on website, bookmark, colleague, etc)
• as detailed a description of the problem as possible
• if possible, one or more screenshots showing the problem: the address bar showing the webpage accessed and the step immediately before the problem arises
• any other information that might help us identify the reason for the problem
(e.g. in the event of a problem with SMS authentication: your mobile telecoms provider, the country where the mobile subscription is based, your current location, the last time you requested the SMS, the last time you successfully received it, etc.)
2. If you haven't done so already, register an incident with the EC Helpdesk for the "ACCESS-RIGHTS" team and provide the information listed under the previous point.
This can be done via the EC Central Helpdesk (EC working hours: 8 a.m.- 6 p.m. CET): EC-CENTRAL-HELPDESK@ec.europa.eu
On opening this ticket, you will be assigned a reference number enabling your request to be tracked.
If you send an e-mail to follow up an existing incident, please give the incident reference ("IM00xxxxxxx") in the subject line.
Last update: 09/12/2015 (4.4.2-gsa) | 11 ms | Contact | Privacy Statement | Top

3.5 iam privacy statement



Contact | Privacy Statement English (en)

EUROPEAN COMMISSION AUTHENTICATION SERVICE (ECAS)

EUROPA > Authentication Service > Privacy Statement

Change password My Account Help | Logout

External
Alexandru-Ionut CHIUTA (chiuta)

IAM Privacy Statement

Privacy statement for users registered with the European Commission's Identity Management Service

1. What is the Identity Management Service?

The European Commission's Identity Management Service (IMS) provides a common way for users to register or be registered for access to a number of different Commission information systems or services (referred to hereafter as sites).
You are affected by this privacy statement if you use the European Commission Authentication Service (ECAS) when logging into Commission sites, as it means that you have been registered in IMS.

Users include the Commission's own staff, personnel of other organisations and members of the public.
Registration may occur:

- at the initiative of a user or of the organisation that the user belongs to or represents
- by means of an automatic transfer of information from the user's organisation to the Commission
- by means of direct entry of the relevant information by the user

IMS includes facilities for authenticating registered users and controlling their access to Commission sites.

In each case, the personal data that is recorded is governed by Regulation (EC) 45/2001.

IMS falls under the responsibility of the Controller, Mr Stephen Quest, Director General, Informatics DG. Further responsibility lies with each processor of the information.

Individual Commission sites that rely on IMS for commonly required personal data may nevertheless collect additional personal data themselves. This is covered by the sites' own privacy statements.

2. What information do we collect, for what purpose and through which technical means?

In general, registration is required:

- if access to a site is restricted to authorised persons
- if there is a simple need for the site to remember you between visits and adapt itself to your needs or wishes
- to allow you to receive further information that you have requested, such as newsletters and information updates
- to grant you individual privileges that you might request or otherwise be entitled to

We store the information that you provide on the registration form (if you registered yourself) or that your organisation provides directly to us. The information you provide may be made available to Commission sites other than the one for which you originally obtained the account provided that you attempt to access them while logged in using your account. By logging in and accessing accounts you are indicating your consent to the use of the data as described in this statement.

The data obtained from the registration process includes both personal details and, if you are registered as a representative or member of an organisation, details related to your link with that organisation. Personal details include your names, geographical location, areas of interest (with respect to the Commission), e-mail address and telephone number. Concerning your organisation, the details may include its name, the department you work for, your office address, the nature of your relationship with the organisation (e.g. employee), your roles and job title and, in order to avoid creating duplicate records, a unique identifier. Information that is obtained from your organisation is subject to the regulations concerning the transfer of personal data and may be only a subset of that mentioned.

The account that we create contains enough information for us to have reasonable confidence that its subsequent usage is by yourself or someone with access to the information you provided (including the password).

We also store certain additional information (listed below) relating to the activity on the user account that we create for you, so that we can protect both your identity and the integrity of the Commission systems that you access.

The additional information is used to diagnose and resolve problems and to deal with security incidents. Much of it relates to attempts to use an identity and thus to events that occur before a user has successfully authenticated.

The Identity Management Service also stores a list of the access rights granted to you by the Commission for the purpose of granting or denying access to individual sites.

Users can inspect all the data that is maintained about their own account, allowing them to check that their account has not been used, and that attempts have not been made to use it, without their knowledge.

We may collect the following additional data about each user:

- Date and time of
  - most recent successful and unsuccessful authentication
  - last change of password
  - last password reset
- Number of good logins and failed attempts
- Your most recent passwords - to make sure you follow the prevailing security policy regarding password re-use.

When you login and / or change your password, we may record further information in log files, such as the IP address used, in line with the purposes stated above. This information can help in following up any doubtful activity relating to your account. It will **not** be used to monitor your activity, except to allow the removal of the account when no longer used.

Many Commission sites use the European Commission Authentication Service (ECAS) for user authentication: ECAS has a special user interface, independent of the client site and provides a single sign-on experience. Some of the information mentioned here is not relevant for the Commission sites that do not use ECAS – if you never login through ECAS it will therefore not be maintained in your account data. Note that logging in through ECAS always involves a page distinctively marked with the ECAS logo. Each time you login to a site protected by ECAS, the identifier, the site and the time will be recorded in a log file. We do not record the time you spent logged in to a site. However, if you logout of ECAS, which is not normally necessary, the time at which you do so will be recorded.

Note: use of cookies

ECAS uses cookies to allow you to log in to different applications without re-entering your username and password. These cookies contain no personal information whatsoever, merely a pointer allowing the authentication service to find your entry in its own tables. The cookies are 'per-session' cookies, i.e. they are destroyed when you close your browser. If you have chosen the option for your browser not to accept such cookies, you will not benefit from this feature and will have to re-authenticate yourself each time you log in to a different client application of the authentication service.
A persistent cookie may be created for your convenience in order to record your choice of language, and at your discretion, your username. In the absence of this cookie, the default language is English.

3. Who has access to your information and to whom is it disclosed?

By registering yourself, you authorise the disclosure of the details you have entered in the user registration system to any Commission site that you access after having given your username and password. If you were registered by your organisation, your consent is assumed to have been given (implicitly or explicitly) for the transfer of your details.

The details of the activity associated with your account are never passed to any other Commission site by IMS.

The Commission will not divulge your information to third parties outside the Informatics DG with the following exceptions:

- the duly authorised support unit or help desk responsible for the domain in which you are registered
- duly authorised bodies, on a case by case basis: OLAF, internal Commission Security Directorate or disciplinary bodies, the Ombudsman, the EDPS.

To preserve your privacy, you can choose (through an option on the login screen) to be notified whenever a relying party (i.e. a Commission site) requests your identity - you will have the option to cancel the operation before any information is passed. However, this may render the application inaccessible to you. If, having logged in into ECAS, you wish to access sites anonymously, you can do one of the following before connecting to the site in question:

- open a new browser session and use it to access the site
- logout from the authentication service
- disable cookies in your browser options

Note that behaviour varies from browser to browser and may affect the results of these operations.

If you need to access a Commission site that requires you to register and authenticate, but you do not wish it to have access to the details you supplied in order to gain access to another Commission site, we suggest you create a separate account for this purpose. This will require you to provide a distinct e-mail address, which need not be traceable to you personally. Of course, this may deny you access to certain sites which require proof of identity.

Your password is stored only in an irreversible form. Apart from your password, the service administrators can view all of the data pertaining to a particular user. This helps them to perform duties such as helping users with problems and diagnosing suspected security incidents.

4. How do we protect and safeguard your information?

The Commission stores your personal information in secure computers and your information can only be accessed by authorised persons and internal sites.

When you login, the password is always encrypted on the network and is decrypted for checking against the stored password by the authentication service, not by the individual site. All passwords (including previous passwords mentioned above) are stored in a form that permits them to be checked against a supplied value, but their actual value cannot be derived from the stored value.

The details about your user account are available only to yourself and the service administrators.

If you registered yourself directly, you should be aware that anyone with access to read your e-mail may be able to use the account you create and acquire the identity it represents. You are responsible for assessing the risk that this presents to you personally.

Similarly, certain users are allowed to reset their password using e-mail. They should bear in mind that anyone else with access to their e-mail (because of automatic forwarding, delegation or other reasons) will be able to reset the password.

For this reason, in order to perform important business or access sensitive information, the Commission requires more stringent identity checks and your account will need to be set up or transformed specifically for this purpose. You will need to contact the relevant Commission department or a delegated representative in your organisation to achieve this.

If you have any reason to believe that your password has been compromised – for example, if your password appears to have been changed without your knowledge - you should notify your normal support contact or contact the Commission as described on the user registration and authentication pages.

Notes:

In principle, and especially if you have access to sensitive systems, you should never reveal your password to anybody else: it is a secret only you should know. In particular, your ECAS password should only ever be entered on screens showing the approved ECAS logo. Do not enter it if you have doubts about the authenticity of the ECAS site.

When you enter your password, make sure your browser indicates (usually by means of a padlock or other icon) that you are on a secure connection and that you are connected to a Commission site address (e.g. ec.europa.eu, webgate.eu-admin.net).

5. How can you verify, modify or delete your information?

You can verify your account information, including the data recorded about activity on your account, in the pages of either the user registration service or the Authentication Service (ECAS). This excludes information that is only held in log files: if you wish to access your log file entries, you may request it by writing to the Controller at the address given below. A response will be given within a period of six weeks from the date of receipt of the request.

In case of difficulty, you can obtain help by following the contact link below (see point 7).

If you registered yourself in the Commission's system, you will be able to change or remove any personal information on-line. However, if your details were registered through a third party, this may not be possible and you will have to contact that third party in order to have the information changed: you may nevertheless have the information removed by the Commission, but if the third party re-submits this information to the Commission, it will be re-instated.

Since it is collected automatically, it is not possible to modify any of the technical data held by the authentication service, with the exception of the password itself.

6. How long do we keep your data?

The Identity Management Service keeps your data for as long as you are recorded as an active user and for a period of one year thereafter. Data concerning users automatically registered from internal sources (in the Commission and certain other EU bodies) may be kept for as long as it is retained in the source system. If you were registered through a third party, the period of activity will usually correspond to a contractual link with that party or be subject to an expiration date. In other cases, the Commission will consider you active as long as you continue to use your account or until your account expires.

Note that in the case of users who registered with IMS themselves, the period of one year is extended in order to allow the exchange of e-mail with a user. This exchange will provide for the user to request an extension, thus resetting to zero the recorded period of inactivity. In the absence of a response from the user, all personal data will be erased.

Data from the Identity Management Service is backed up regularly by the Commission to ensure a correct system restore if necessary to restart operations. Furthermore, the Identity Management Service is closely monitored and all sensitive actions on the system are logged, including each authentication request. These logs (log files) are rotated regularly and removed from the active system after a maximum of six months in accordance with REGULATION (EC) No 45/2001. All log files backed up by the standard Commission's backup procedure will not be removed from back-up tapes until those tapes are recycled, but that log data will not be restored if system restore is required.

7. Contact Information

If you wish to ask questions or post complaints about the service with respect to the use of your personal information, you should follow the contact link that is shown on each Identity Management service page or write to the following address:

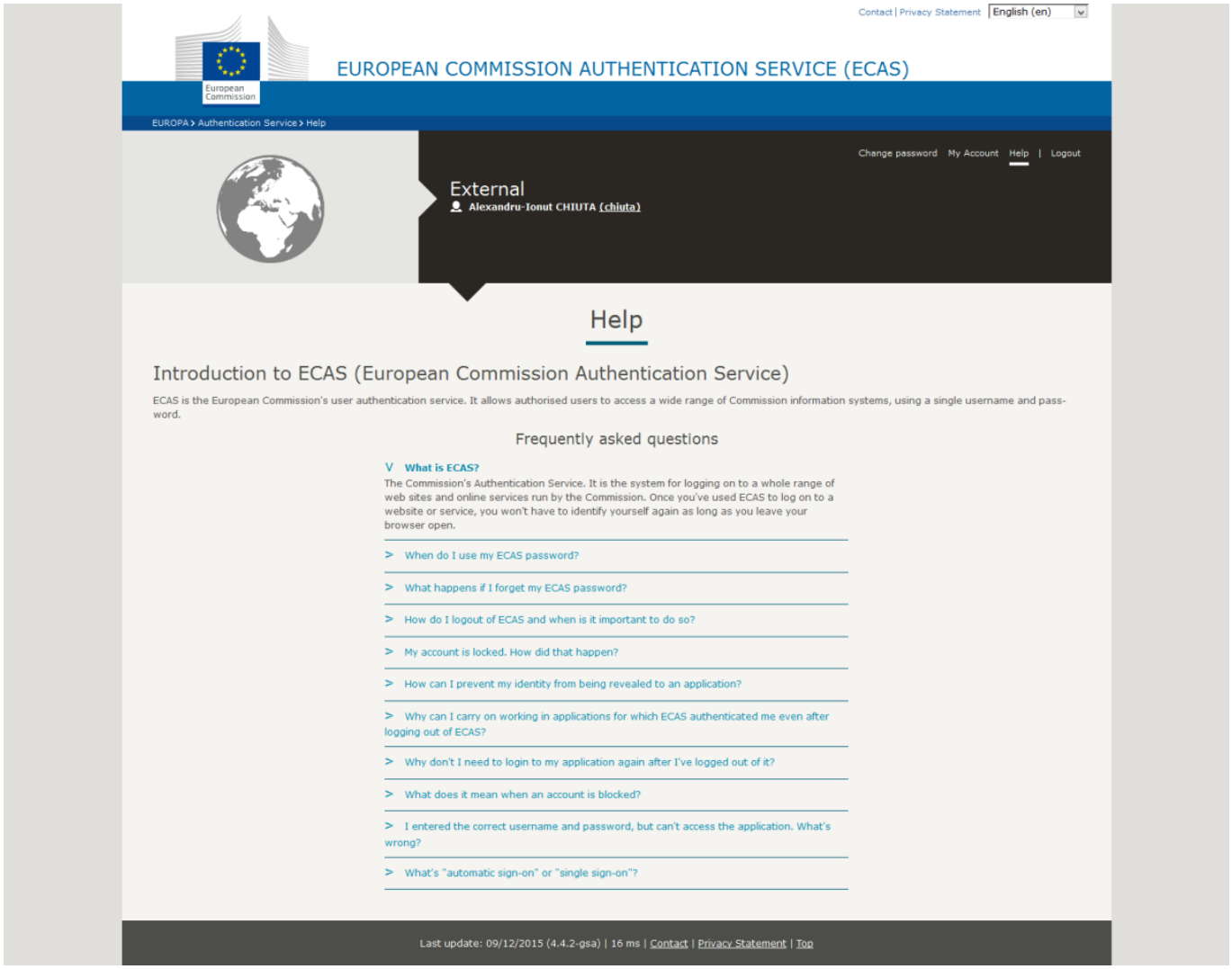
> The Director General
> Informatics DG
> European Commission
> 200 rue de la Loi
> B-1040 Brussels

8. Recourse

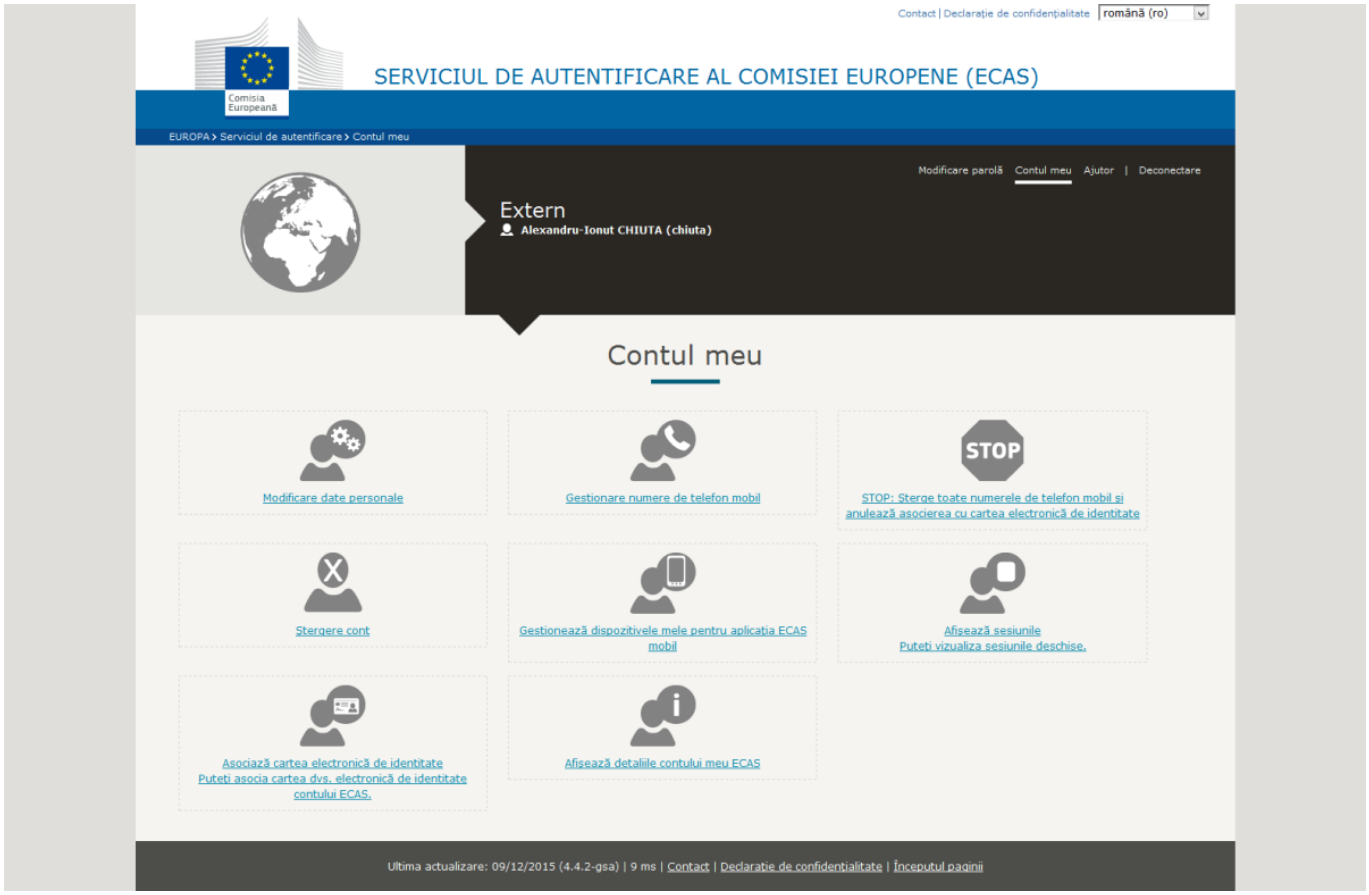
If necessary, complaints can be addressed to the European Data Protection Supervisor.

Last update: 09/12/2015 (4.4.2-gsa) | 18 ms | Contact | Privacy Statement | Top

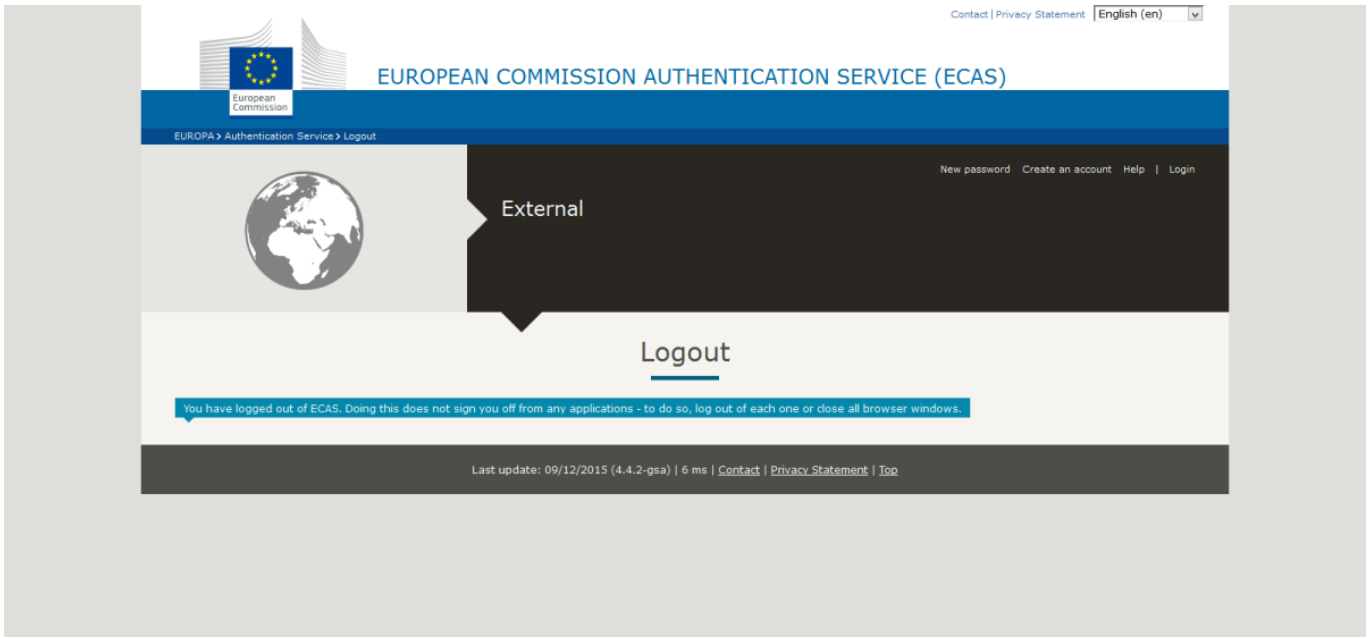
3.6 help



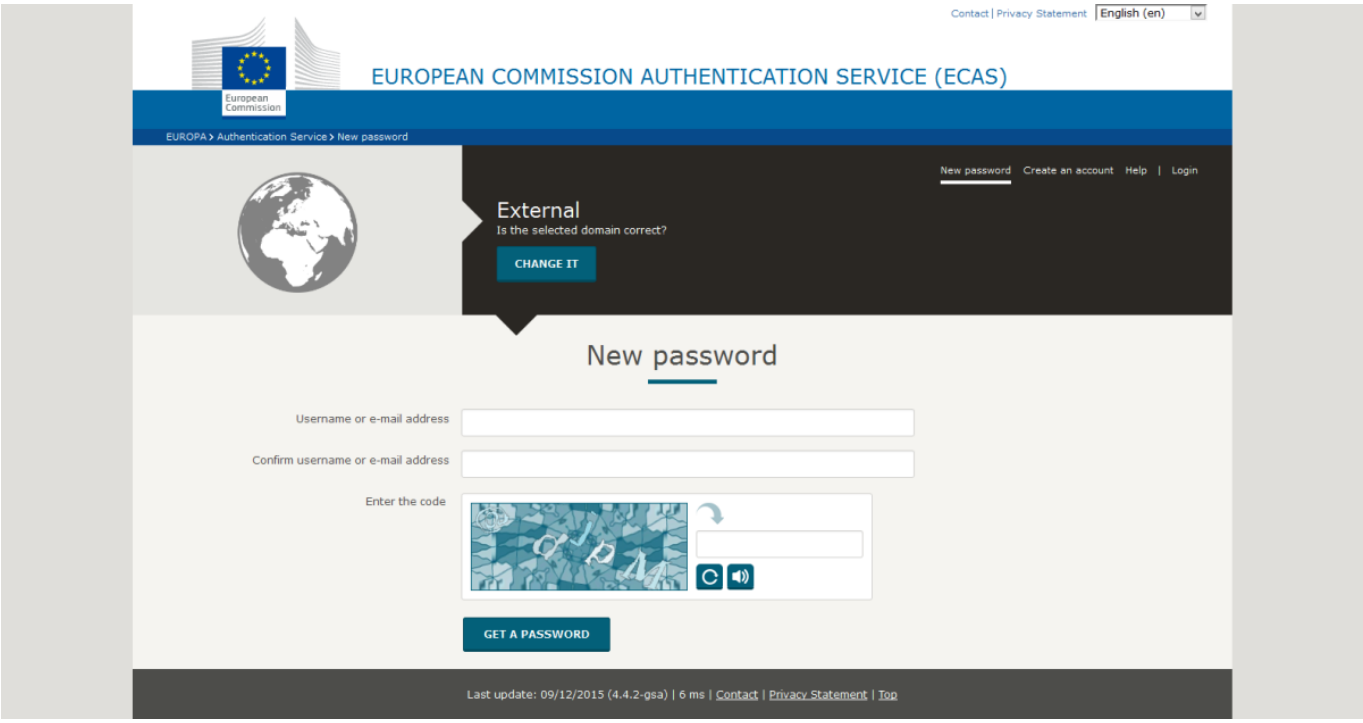
3.7 contul meu



3.8 logout



3.9 lost your password new password



From:
https://cnred.link/imipqnet/ - **IMI PQ NET România**

Permanent link:
https://cnred.link/imipqnet/doku.php?id=ro:materiale:prezentari:serviciul_de_autentificare_al_comisiei_europene_ecas

Last update: **2020/08/01 09:14**