UniWeb

New access credentials and qualified signature certificates on remote server

Sommario

1 Process description

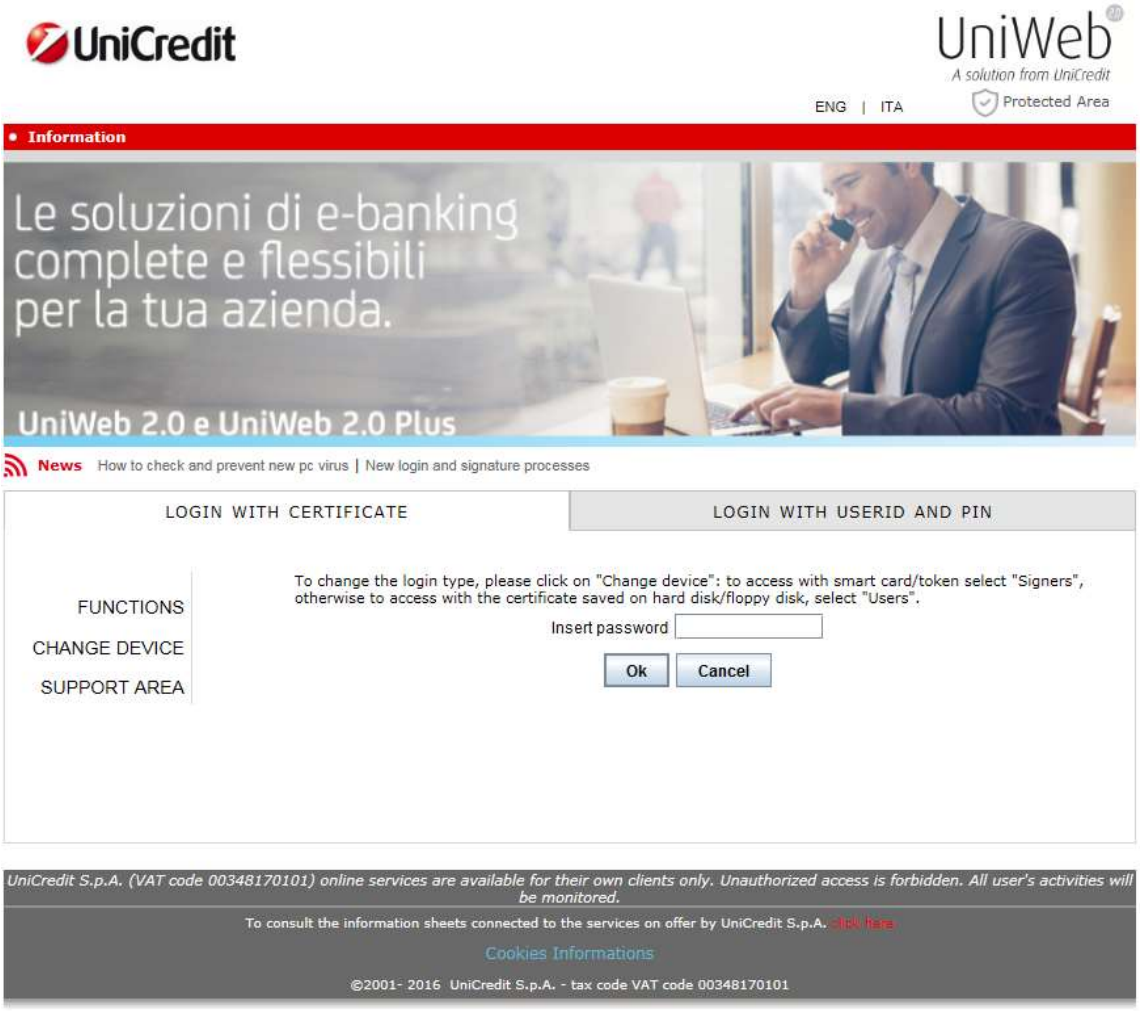
UniCredit, while evolving its e-Banking products for Corporate customers, started a process of conversion of existing UniWeb users' accounts.
The enhancement implies the elimination of Java Applets in Login, Signature and Upload/Import processes, so it will no more be needed to have Java installed on the machine used to connect.

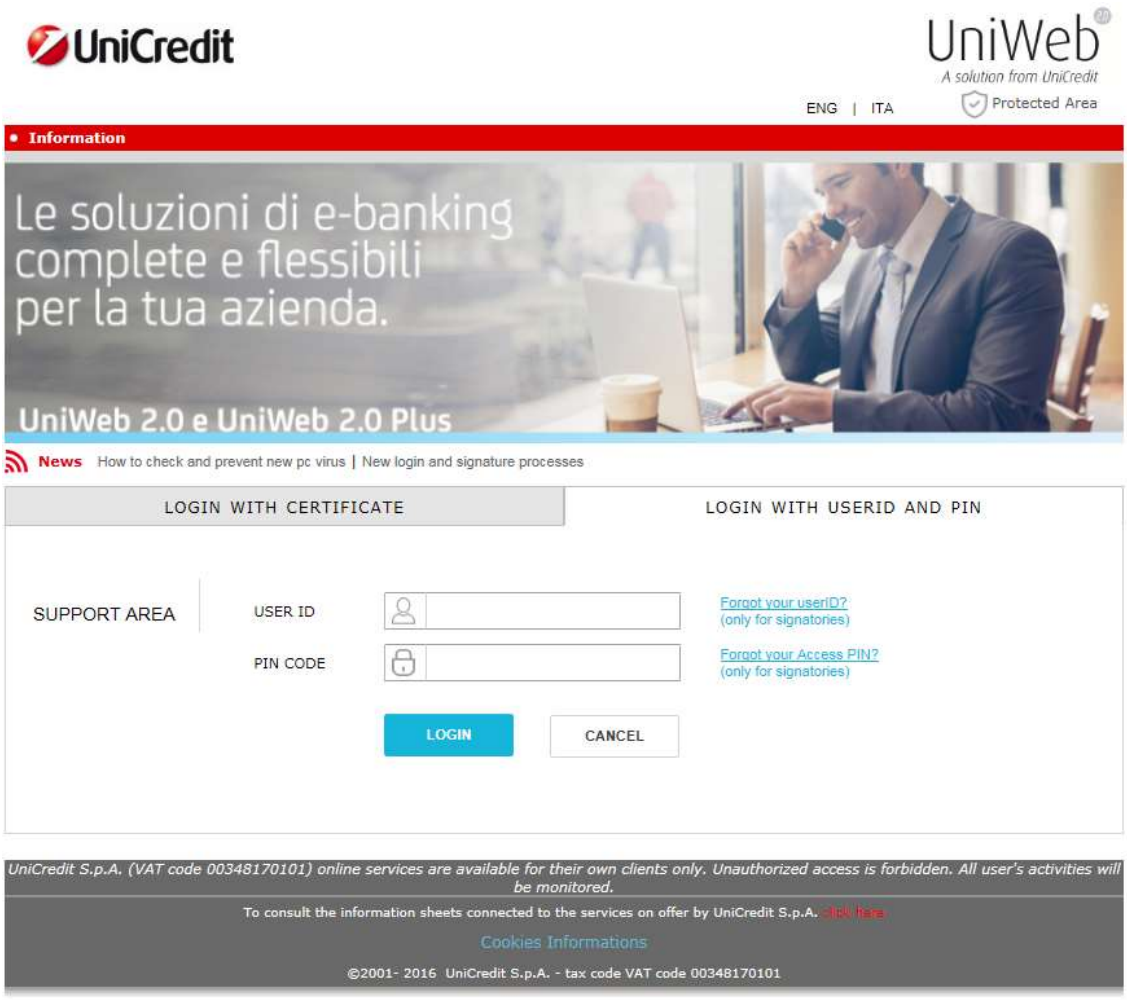
Login and Signature processes will be simpler and more efficient, while Upload/Import processes will keep the current aspect and functionalities.

In details after migration or registration:

1. Users' access will happen through the insertion of an userID, assigned by the system during registration or during migration, and an Access PIN chosen by the owner of the account during first access (when he/she will have to change the single-use PIN received during registration) or during migration
2. For signatories the signature of every transaction / online document will happen through the insertion of an OTP (One Time Password) generated by one of the security devices that every signatory must have, The signature will be imprinted through a qualified signature certificate on remote server that will be generated at first access, during migration or during the lifecycle of the signatory, according with needs and contingencies

Migration of existing accounts will happen progressively, so it is planned a period of time in which users who login and sign with the old rules and users already in the new context will coexist.
To allow the coexistence the login page has been split with two Tabs corresponding to the two login methods, as shown in the following image.





Users already provided with userID and Access PIN cannot access with the old login method or sign with old certificates, in other words the migration is irreversible.
The insertion of 4 consecutive wrong Access PINs leads to the lock of the userID which can be unlocked autonomously by signatories and asking to their Administrator of Operating Company Profiles for the users.

2 Migration logics

2.1 Pre-requisites

The prerequisites to access to migration procedure are the following ones:

- Users → to be provided of working access credentials
- Signatories → to be provided of working access credentials and an OTP generator security device
- Administrators of Operating Company Profiles → to be provided of working access credentials and an OTP generator security device

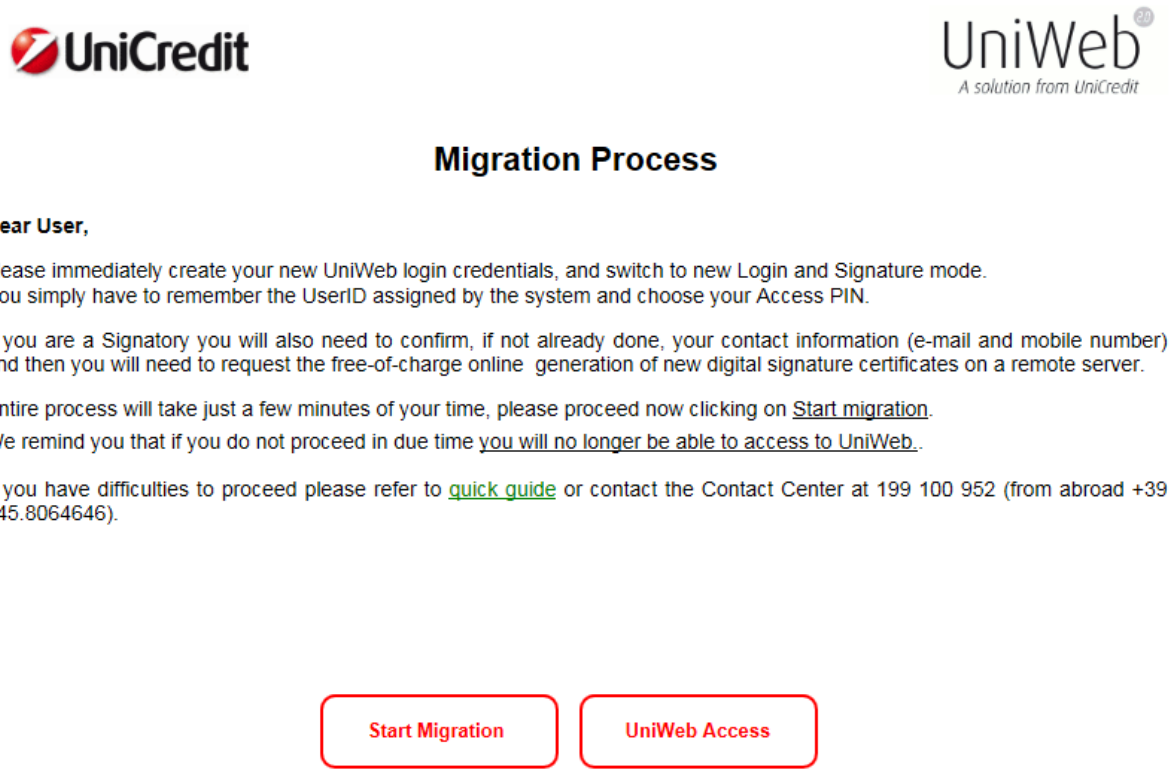
Last two profiles must have an OTP generator to start the migration, so it is mandatory that they ask it before the start of their migration, if not already done.

2.2 Migration calendar

Users subject to migration will be divided in migration “lots” to distribute them on the whole period of time plannd for the process (from October 2016 until April 2017), and the migration will be suggested by the system to the users just after the login, once their lot’s start date has come.
Administrators of Operating Company Profiles will receive by e-mail a notification seven days before the start date of the migration lot where the users (signatories and users) that they administer are planned to migrate.

Every lot will have an approximate duration of thirty days and the users who didn’t completed the migration:

- During the duration of the lot: after login (and after possible REB selection for multi-REB signatories) the users will see an information page that describes roughly the process and allows to start immediately the migration (recommended choice) or to proceed with UniWeb access postponing the migration to another moment. The page is shown hereafter:



- After the end date of the lot: after login (and after possible REB selection for multi-REB signatories) the users will see the same previous information page that will allow only to start immediately the migration. It is no more possible to access to UniWeb without migration. The page is shown hereafter:

UniCredit

UniWeb
A solution from UniCredit

Migration Process

Dear User,

please immediately create your new UniWeb login credentials, and switch to new Login and Signature mode.
You simply have to remember the UserID assigned by the system and choose your Access PIN.

If you are a Signatory you will also need to confirm, if not already done, your contact information (e-mail and mobile number) and then you will need to request the free-of-charge online generation of new digital signature certificates on a remote server.

Entire process will take just a few minutes of your time, please proceed now clicking on Start migration.
We remind you that if you do not proceed in due time you will no longer be able to access to UniWeb..

If you have difficulties to proceed please refer to quick guide or contact the Contact Center at 199 100 952 (from abroad +39 045.8064646).

Start Migration

For signatories only it will be mandatory the use of OTPs to validate some migration steps; the signatories who haven't it will see after a login, before the end of their lot, an information page that notifies this situation and remind them to request a security device to the bank, leaving only the possibility to proceed.

UniCredit

UniWeb
A solution from UniCredit

Migration Process - Security device not found

Dear Signatory,

to create your new UniWeb login credentials, and switch to new Login and Signature mode, you must request an One-Time Password (OTP) generator device.
Please quickly proceed with your request, online or by contacting your Branch or your Relationship Manager.

We remind you that after {migration end date} you will no longer be able to proceed online and you will need to contact your Relationship Manager or your Branch, otherwise you will no longer be able to access to UniWeb.

If you have difficulties to proceed please refer to quick guide or contact the Contact Center at 199 100 952 (from abroad +39 045.8064646).

UniWeb Access

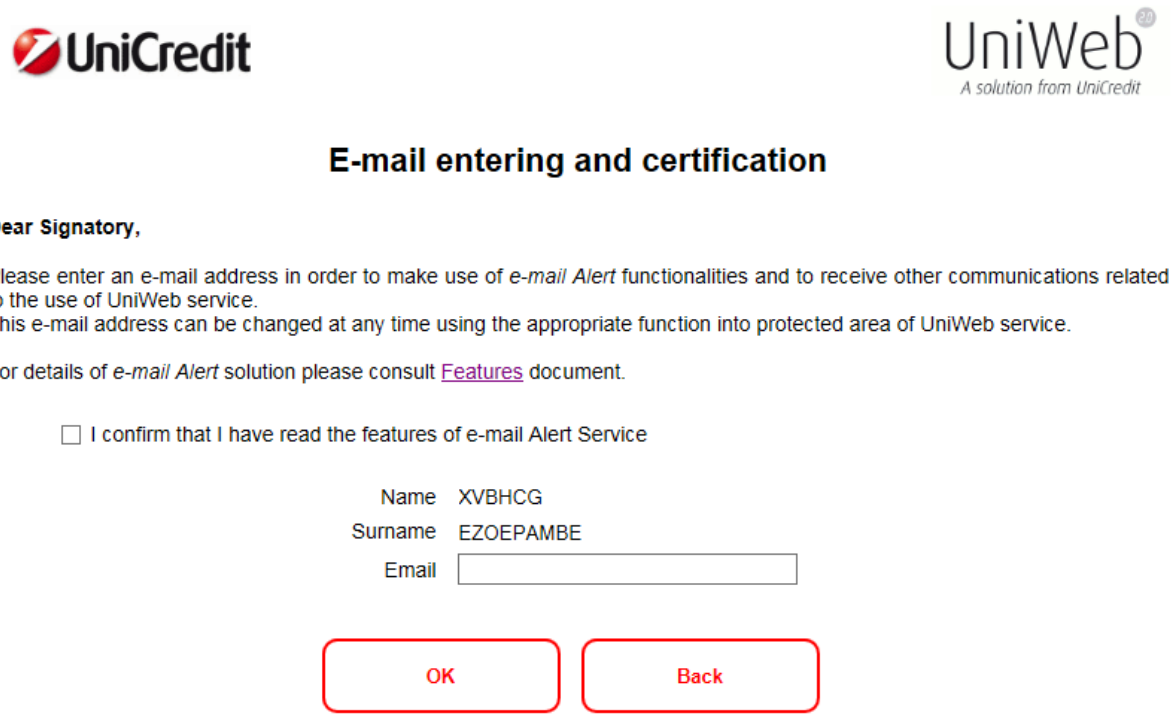
The duration of a migration lot does not imply that users must migrate in that period of time, but it means only the period when the use can still postpone the migration.
An user (signatory or user) who should access (with the pre-migration logics) after the end date of his/her migration lot, will anyway be allowed to start the migration, but he/she will not be allowed to login to UniWeb until he/she will not have obtained the new credentials (userID and Access PIN).

2.3 Migration steps

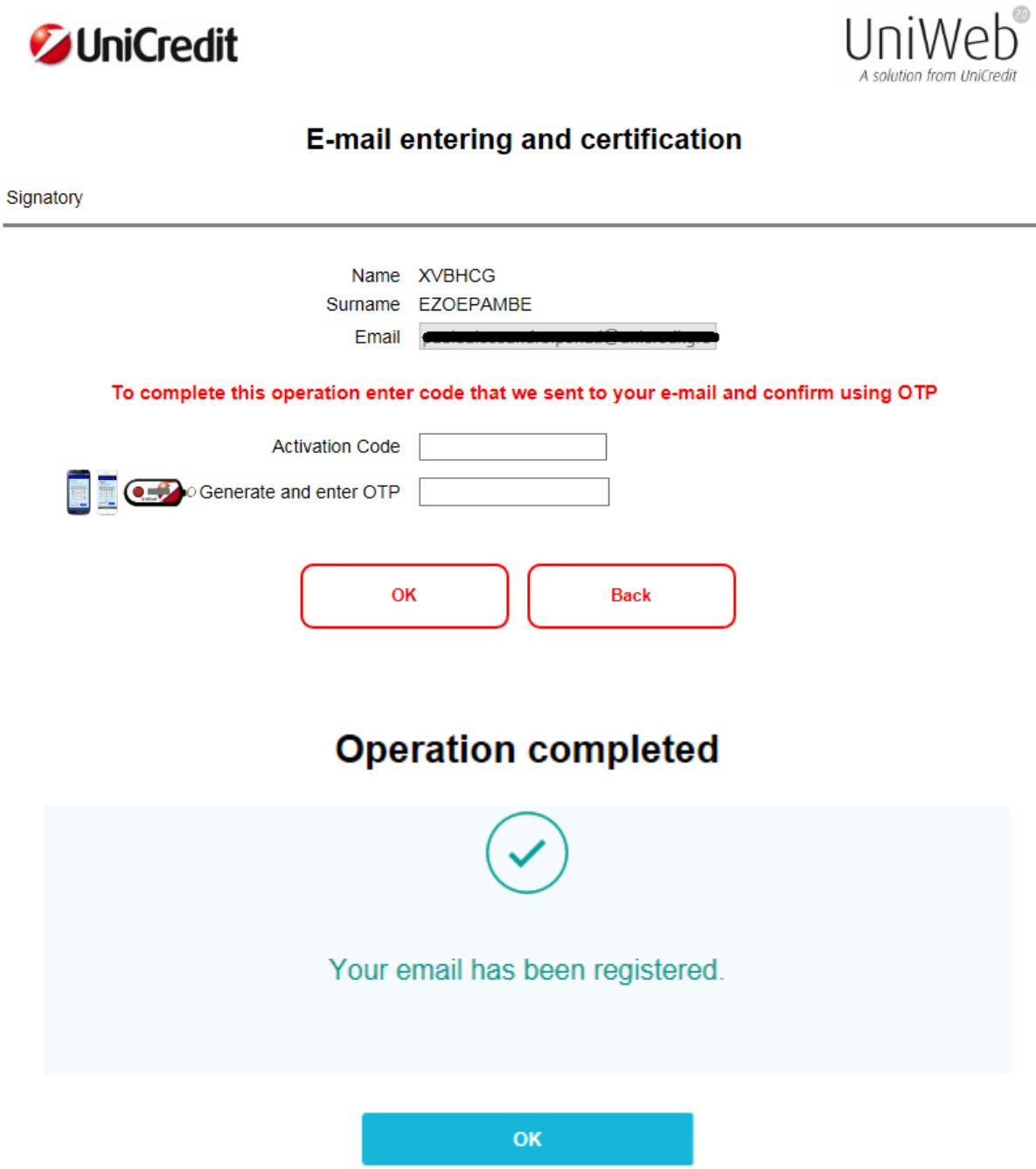
Migration process implies a set of steps for the user described in the following paragraphs. Among parentheses it is shown the kind of users they are referred to.
The full one time process requires only a few minutes to be completed.

2.3.1 e-mail certification (*only signatories without certified e-mail Alert*)

Signatories who does not have at least one certified e-mail address for e-mail Alert service for the REB in use are asked to insert one using the following page:



The e-mail certification happens as usual by means of the sending from UniWeb of a five digits verification code to the e-mail chosen by the user.
Signatory must insert this code in the following page to confirm to have the access to that e-mail address and to avoid mistyping, confirming the operation with an OTP.



2.3.2 **Mobile phone number certification (*only signatories without certified mobile phone number*)**

Signatories who does not have a certified mobile phone number are asked to insert one using the following page:

Mobile Number entering and certification

Dear Signatory,

Please enter a mobile number that can be used by the Bank to contact you if it will be needed to verify the authenticity of your transactions, for your protection and for protection of your operations.

This mobile number can be changed at any time using the appropriate function into protected area of UniWeb service.

Name	XVBHCG
Surname	EZOEPAMBE
Country	Italia(+39)
Mobile Number	[redacted]

OK Back

The mobile phone number certification happens as usual by means of the sending from UniWeb of a five digits verification code by SMS to the mobile phone number chosen by the user.
Signatory must insert this code in the following page to confirm to have the access to that mobile phone number and to avoid mistyping, confirming the operation with an OTP.

Mobile Number entering and certification

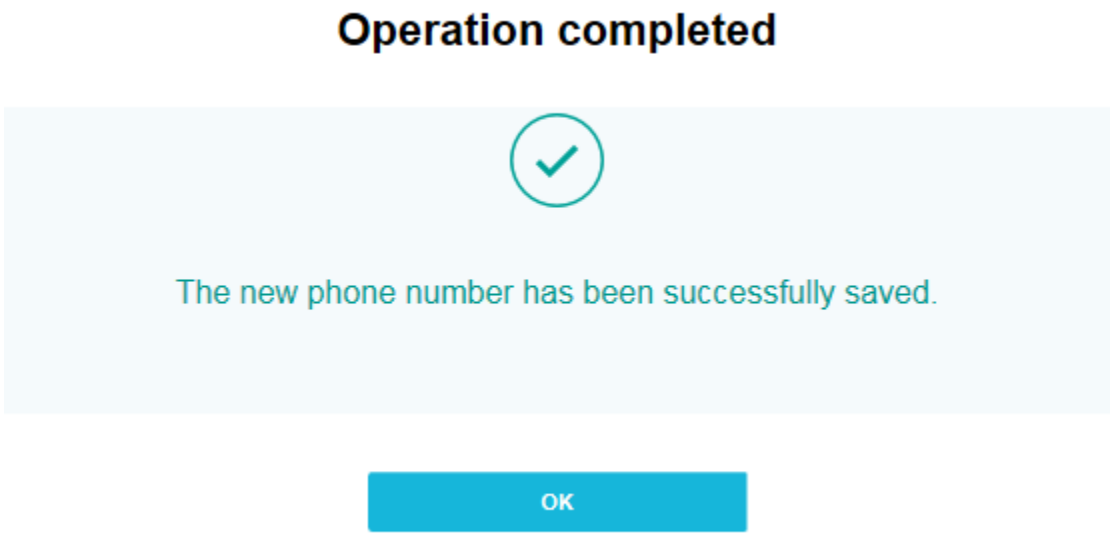
Signatory

Name	XVBHCG
Surname	EZOEPAMBE
Mobile Number	[redacted]

To complete this operation enter code that we sent to your mobile number via SMS and confirm using OTP

Activation Code	
 Generate and enter OTP	

OK Back

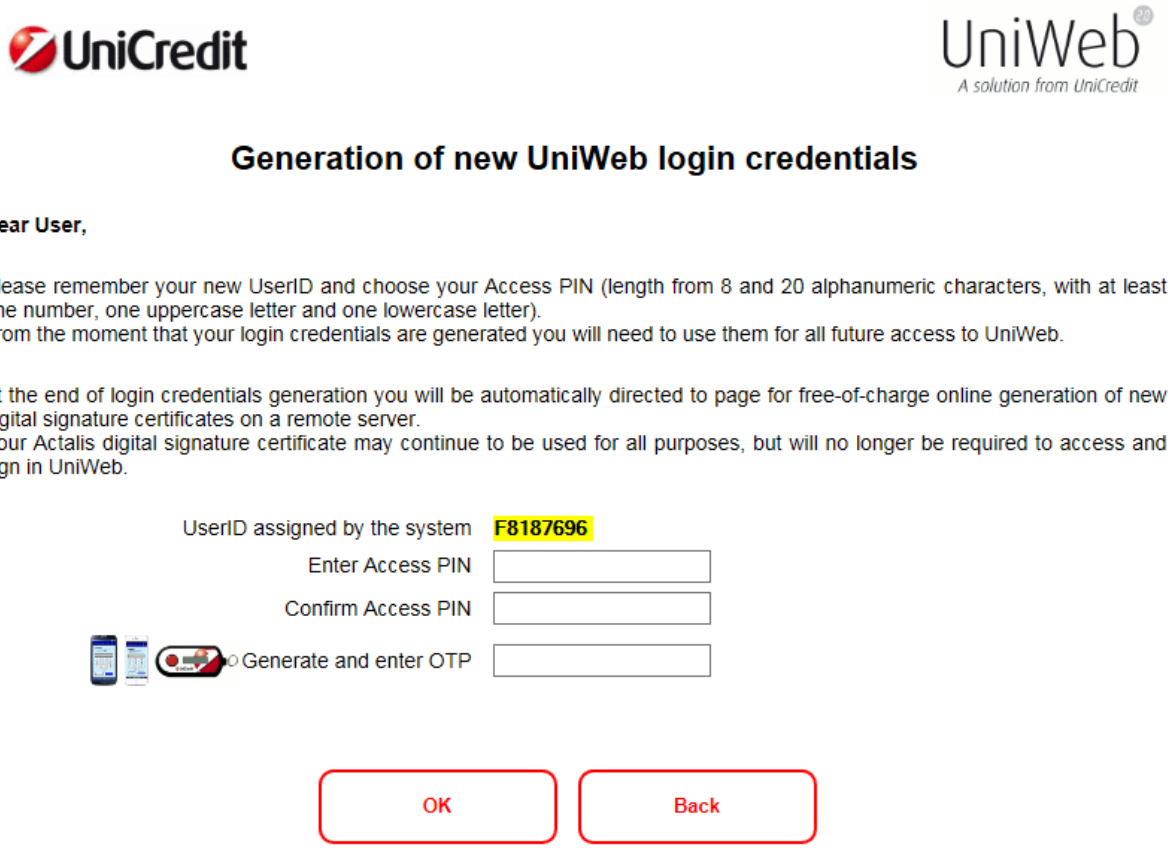


2.3.3 **Registration of new access credentials**

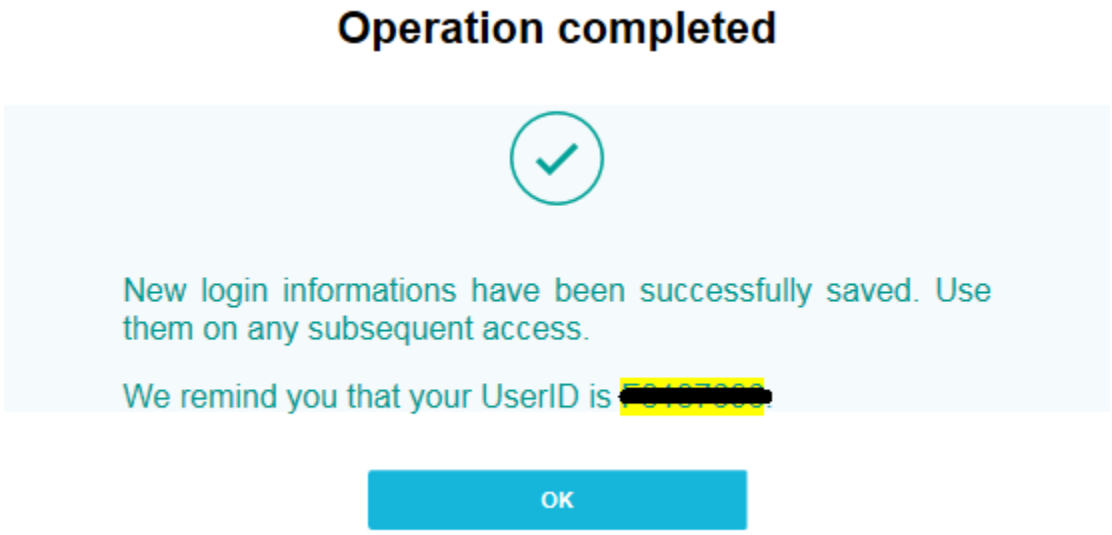
The following page is displayed to users (users and signatories) and they can find in it the userID assigned by the system (to be remembered and that cannot be changed in the future), and they must choose their Access PIN, inserting it twice to avoid mistyping. Access PIN must comply with following rules:

- From 8 to 20 alphanumeric characters (A-Z, a-z, 0-9)
- At least a number
- At least an uppercase letter
- At least a lowercase letter

Signatories must confirm the data inserted with an OTP, while the users must simply confirm it pressing the OK button.
The new credentials generation page presented to signatories is shown hereafter:



After the confirmation of the new credentials, users can proceed to UniWeb, having finished their migration process. Since that moment the new credentials must be used in every login to UniWeb.

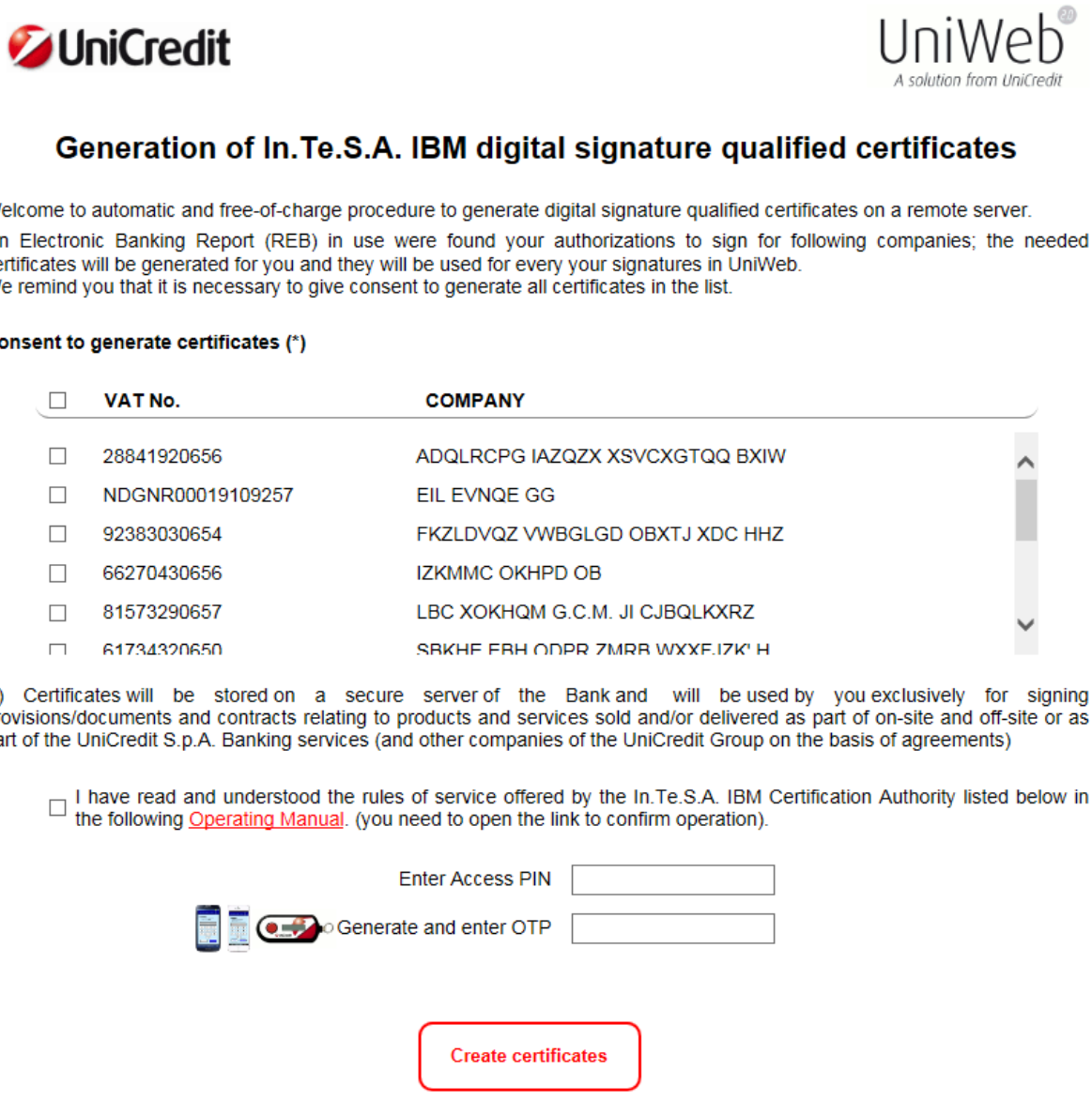


For multi-REB signatories the credentials are valid for the access to every REB they are enabled to work for. Signatories, after the generation of the new credentials, must still generate the qualified signature certificates (free of charge) for every company of the REB in use, the process is described in the following paragraph.

If for any reason the signature certificates generation process does not finish correctly, then the signatory has anyway completed the credentials generation, and since then they must be used in every login to UniWeb.
The unfinished signature certificates generation process is proposed again at the following login to UniWeb.

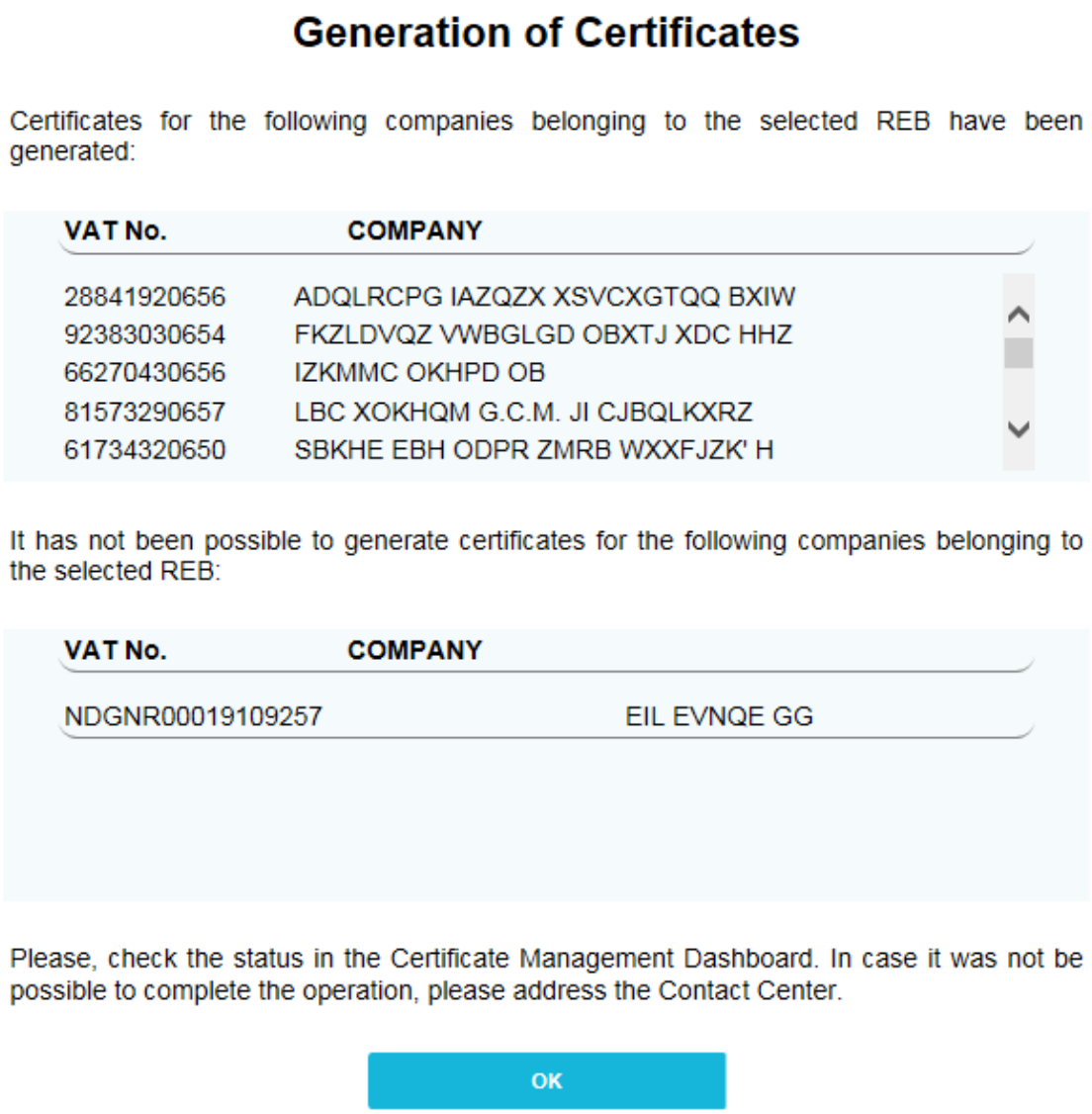
2.3.4 One time generation of new qualified signature certificates on remote server (*signatories only*)

The following page is displayed to signatories and they can find in it the list of the companies of the REB in use they are enabled to sign for:



The signatory, in order to proceed, must select all the listed companies, open the Certification Authority's Operating Manual link, and select the checkbox to confirm to have read it, inserting his/her Access PIN and an OTP to confirm the operation.

Once ended the certificate generation process (the system displays the progress with the number of generated certificates and the number of the missing ones to the end of the process) the migration is finished for that REB and the signatory proceeds to the welcome page of UniWeb, being fully operational in the new context.



If the signatory is profiled to work on more than one REB, then he/she will see another one time page to generate the certificates for the companies he/she is enabled for that REB to sign for, when logging in for the first time (with userID and Access PIN) with another REB.

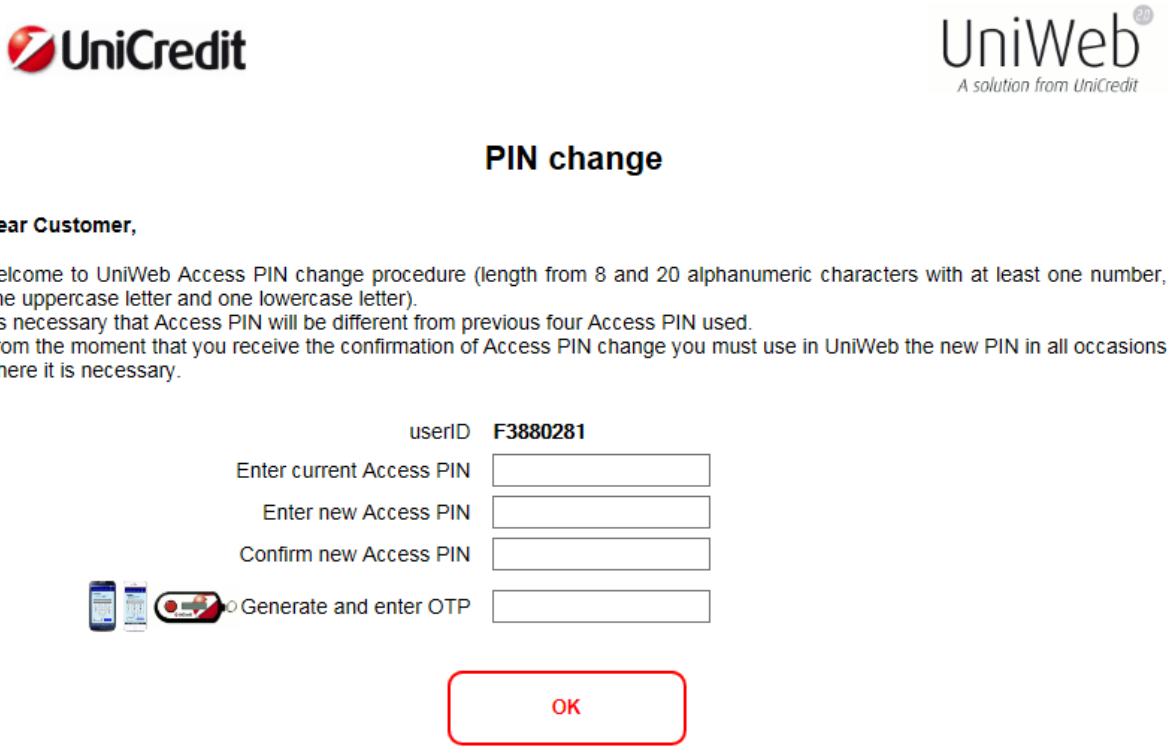
3 First access of users registered with userID and Access PIN

User already registered with the new credentials (userID and Access PIN) must perform some simple configuration steps at the first login to UniWeb, which can be done a few minutes after the registration of the user in the Bank.
The full one time process requires only a few minutes to be completed.

3.1 Change of the single use Access PIN

During the registration the users are provided by single use five digits Access PIN (signatories receive it from the bank in a secret envelope, while users receive it from the Administrator of the Company Operating Profiles).

This PIN must be mandatorily changed at first access using the following page, where it is displayed the userID that the system assigned to the user, who must insert the single use PIN received and choose his/her new Access PIN, inserting it twice in order to avoid mistyping.



Access PIN must comply with following rules:

- From 8 to 20 alphanumeric characters (A-Z, a-z, 0-9)
- At least a number
- At least an uppercase letter
- At least a lowercase letter
- Different from last three formerly used by the signatory/user

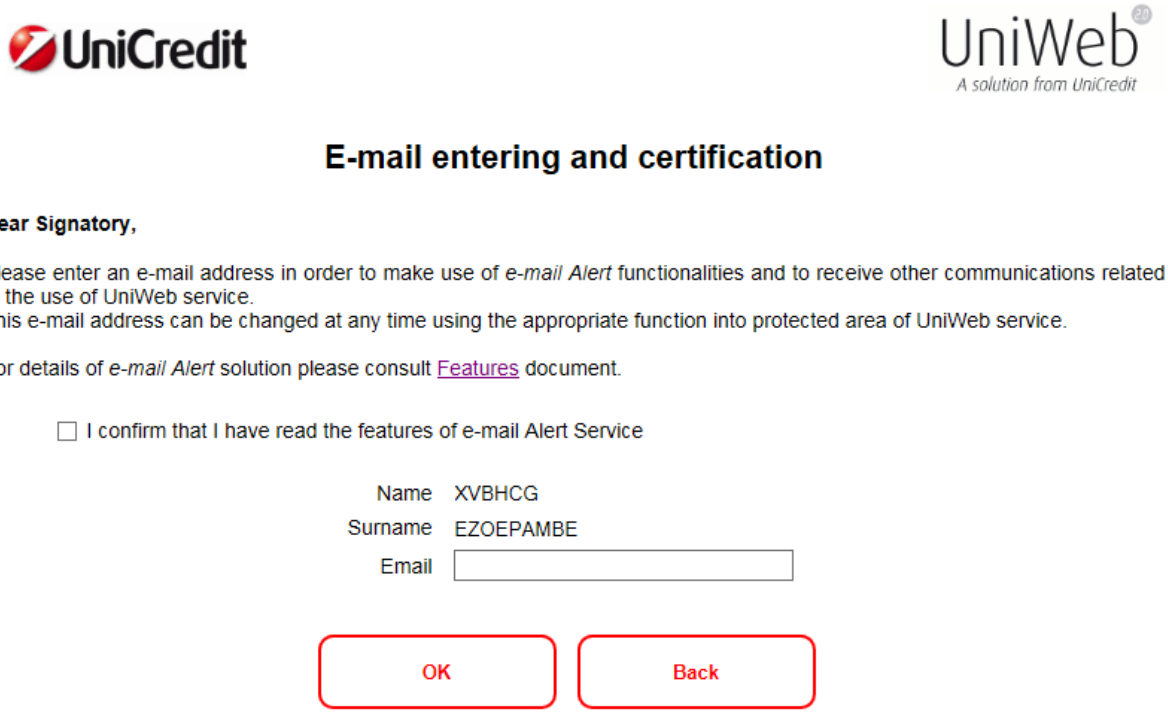
Signatories must validate the inserted data with an OTP, while users must simply confirm it pressing the OK button.

After the confirmation of the new credentials, users can proceed to UniWeb, having finished their configuration process. For multi-REB signatories the credentials are valid for the access to every REB they are enabled to work for. Since that moment the new credentials must be used in every login to UniWeb.

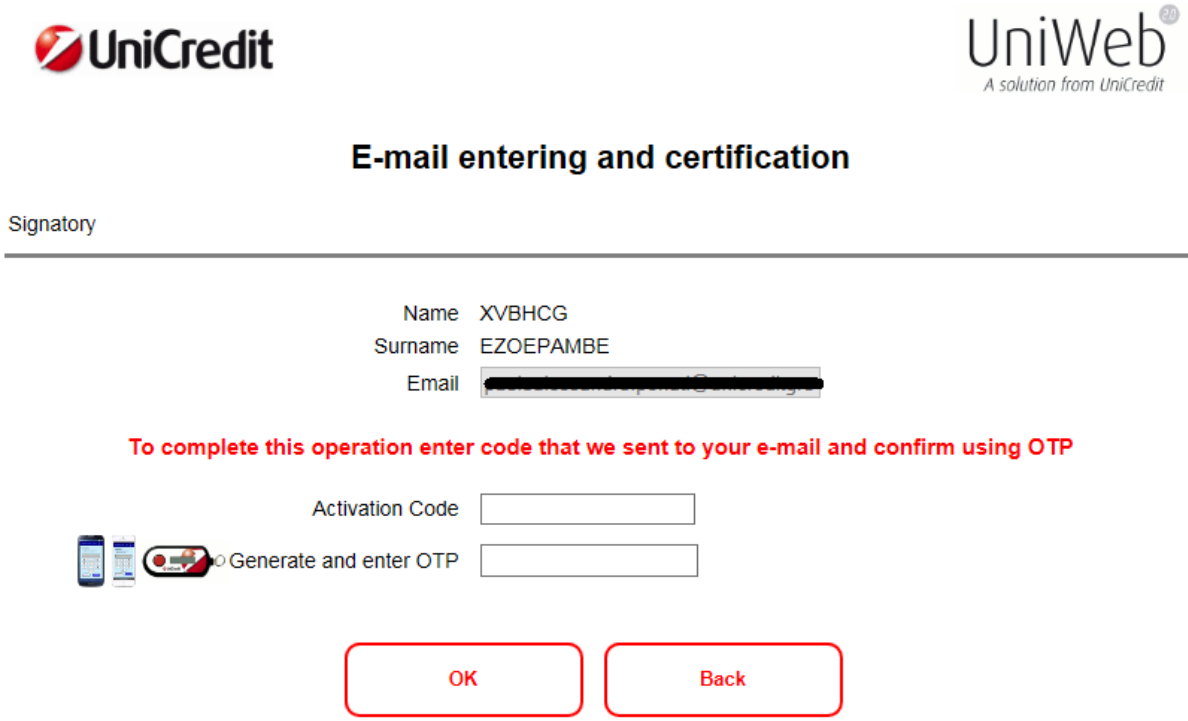
Signatories, after the change of the Access PIN, must still perform some configuration steps described in the following paragraphs.
If for any reason the following steps do not finish correctly, then the signatory has anyway completed the credentials configuration, and since then they must be used in every login to UniWeb.
The unfinished process steps are proposed again at the following login to UniWeb.

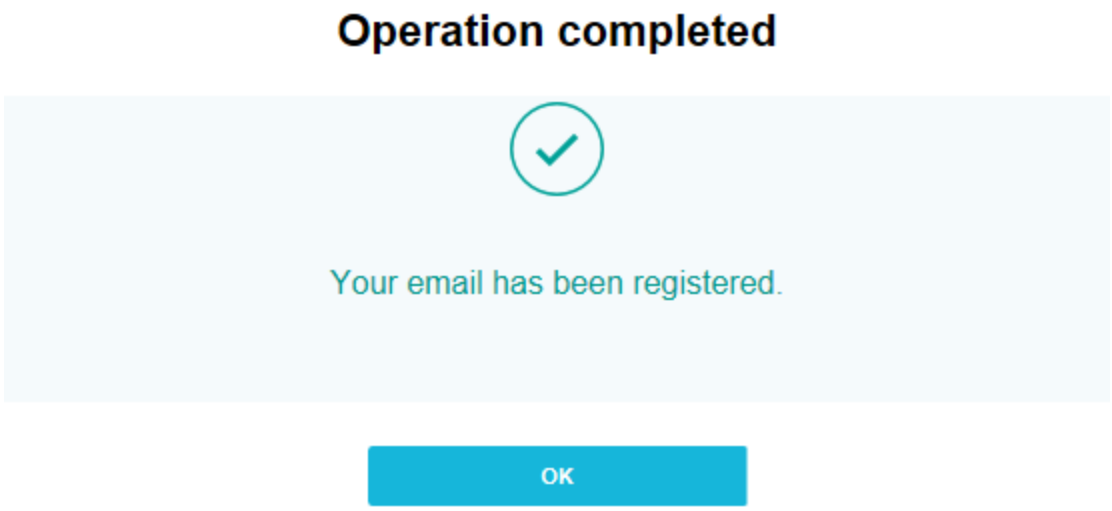
3.2 e-mail certification (*signatories only*)

Signatories are asked to insert one certified e-mail address for e-mail Alert service for the REB in use using the following page:



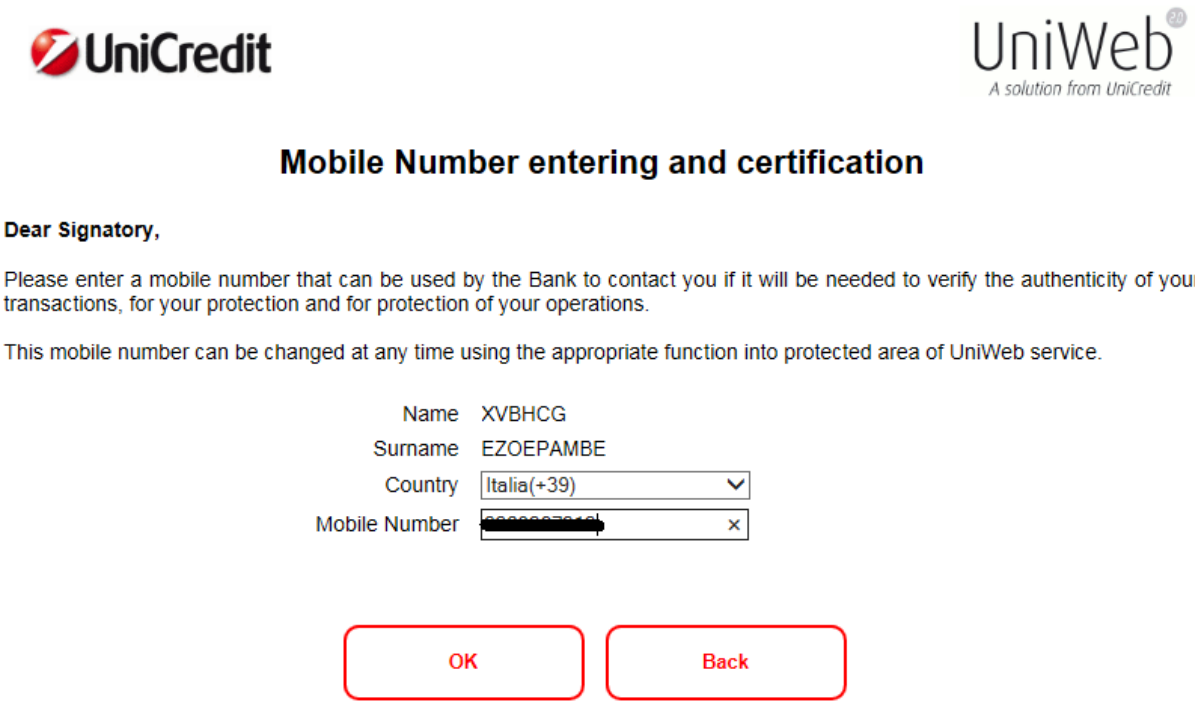
The e-mail certification happens as usual by means of the sending from UniWeb of a five digits verification code to the e-mail chosen by the user.
Signatory must insert this code in the following page to confirm to have the access to that e-mail address and to avoid mistyping, confirming the operation with an OTP.



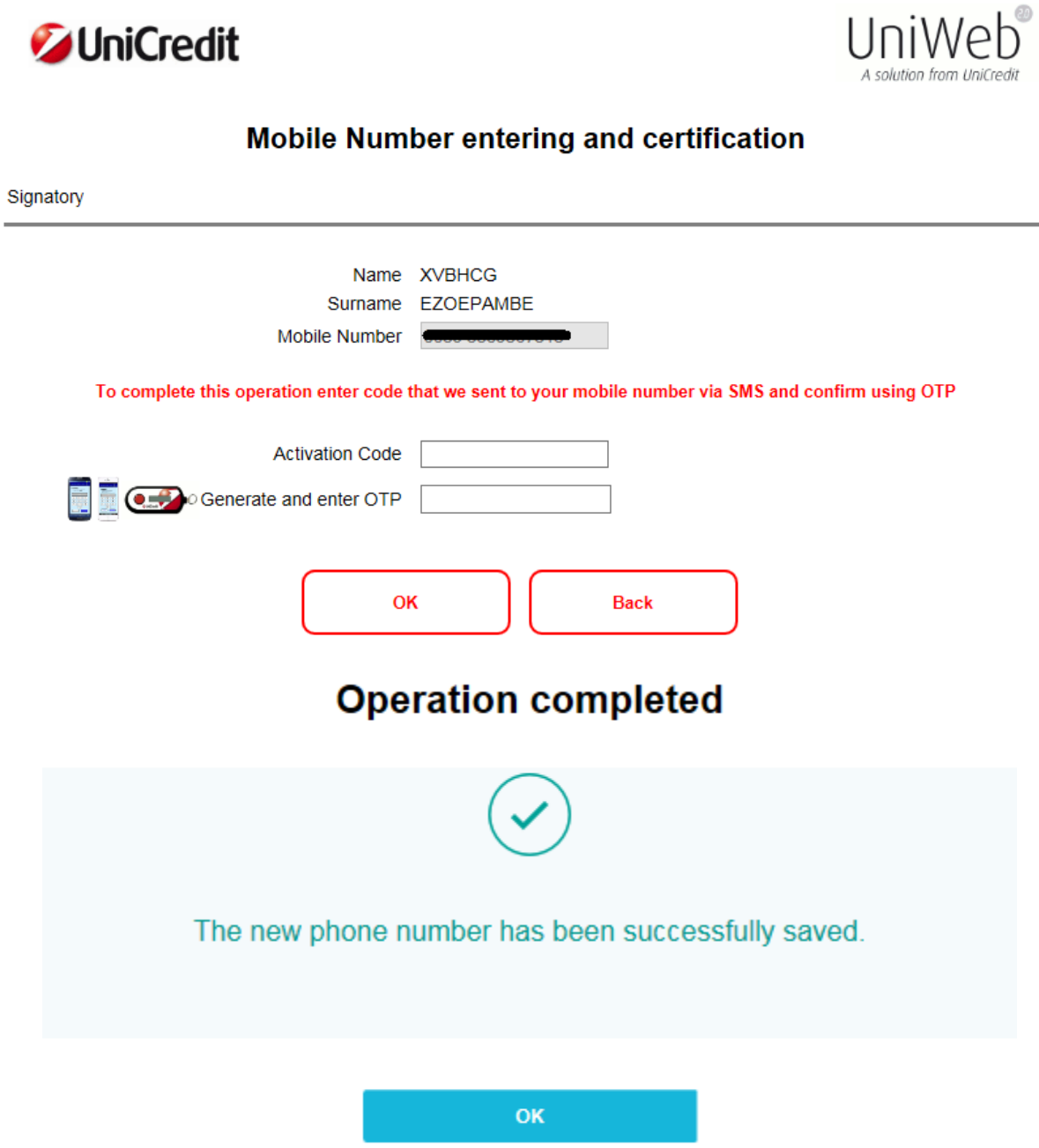


3.3 Mobile phone number certification (*signatories only*)

Signatories are asked to insert a certified mobile phone number using the following page:

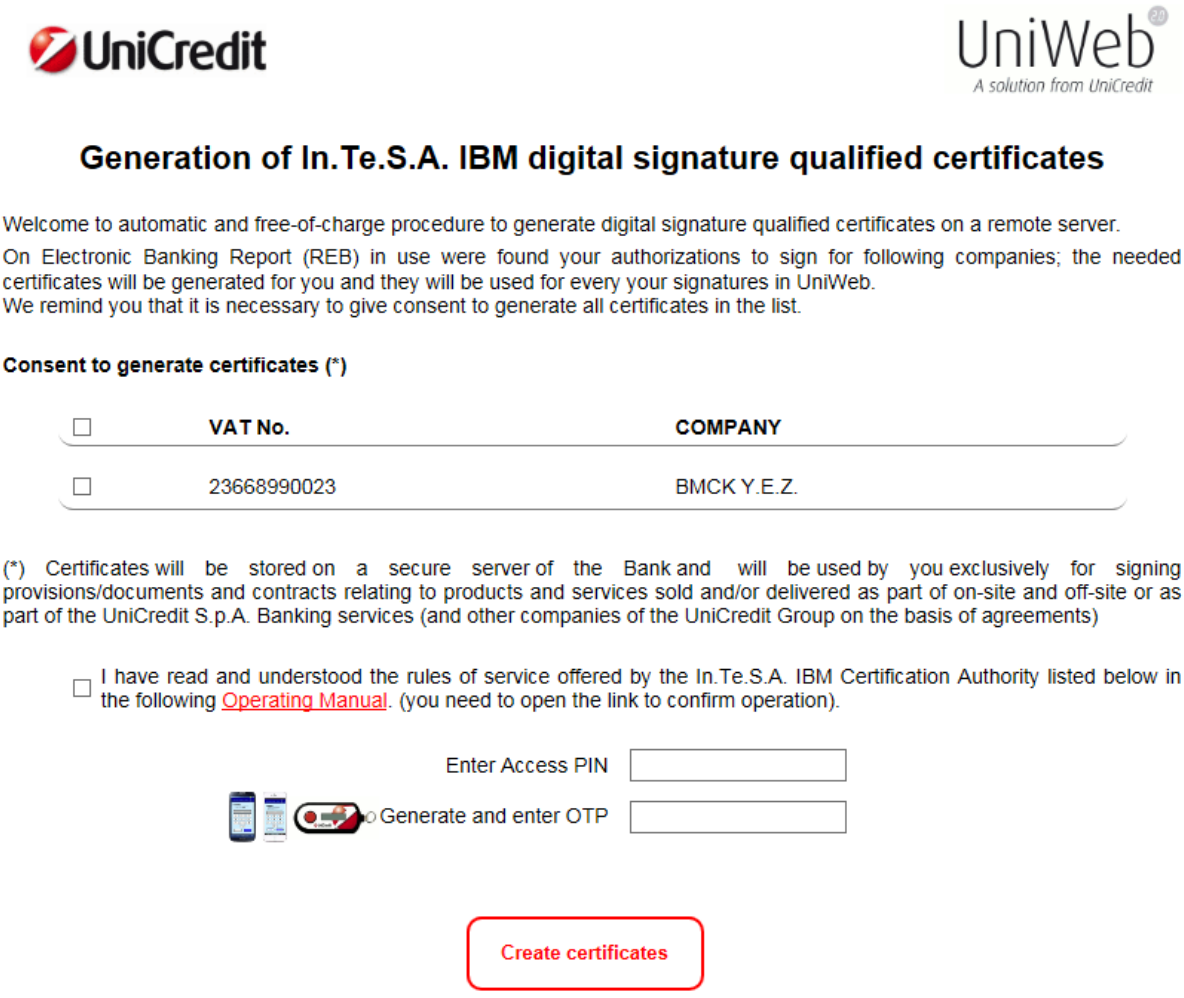


The mobile phone number certification happens as usual by means of the sending from UniWeb of a five digits verification code by SMS to the mobile phone number chosen by the user.
Signatory must insert this code in the following page to confirm to have the access to that mobile phone number and to avoid mistyping, confirming the operation with an OTP.



3.4 One time generation of the new qualified signature certificates on remote server (*signatories only*)

The following page is displayed to signatories and they can find in it the list of the companies of the REB in use they are enabled to sign for:



The signatory, in order to proceed, must select all the listed companies, open the Certification Authority's Operating Manual link, and select the checkbox to confirm to have read it, inserting his/her Access PIN and an OTP to confirm the operation.

Once ended the certificate generation process (the system displays the progress with the number of generated certificates and the number of the missing ones to end the process) the system shows a message to confirm that the migration is finished for that REB and the signatory proceeds to the welcome page of UniWeb, being fully operational in the new context.

If the signatory is profiled to work on more than one REB, then he/she will see another one time page to generate the certificates for the companies he/she is enabled for that REB to sign for, when logging in for the first time (with userID and Access PIN) with another REB.

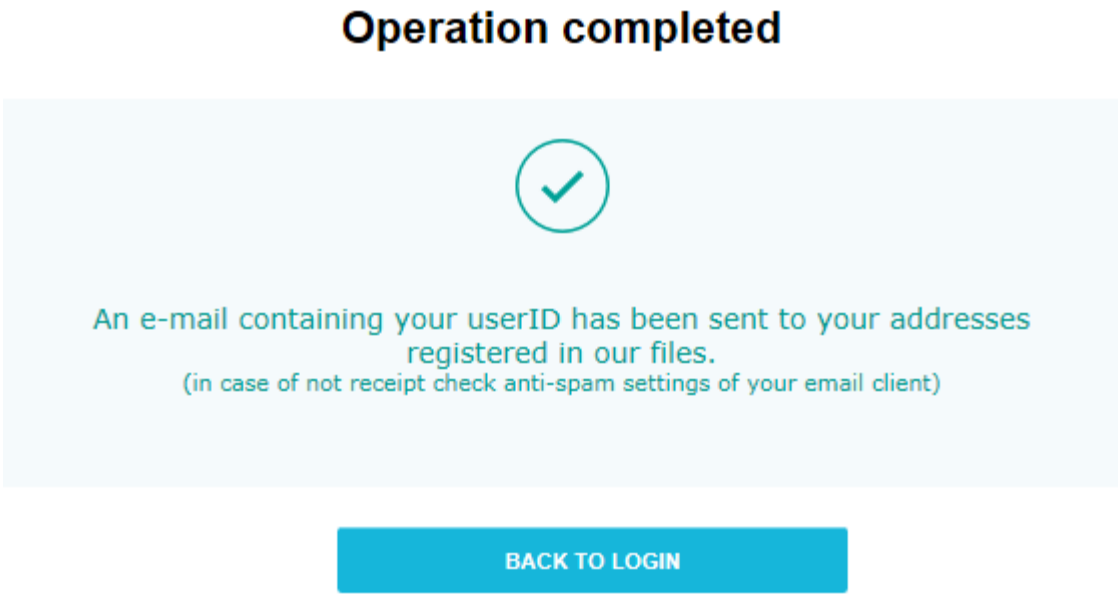
4 User account administration functionalities

Users already with the new credentials (userID and Access PIN) can manage credentials and qualified signature certificates on remote server by means of some new UniWeb functionalities.
Some of these functionalities (as pointed out in the parentheses) are reserved to signatories only.

4.1 UserID recovery *(signatories only)*

On UniWeb login page the signatories can ask the sending of their userID (e.g. in case they forgot it) to the e-mail addresses registered for e-mail Alert service.
The link on the login page brings to the following page where the signatory must insert his/her fiscal code, confirming the request with an OTP.

The system proceeds to send the user ID by e-mail to the e-mail addresses registered for e-mail Alert service for that signatory.

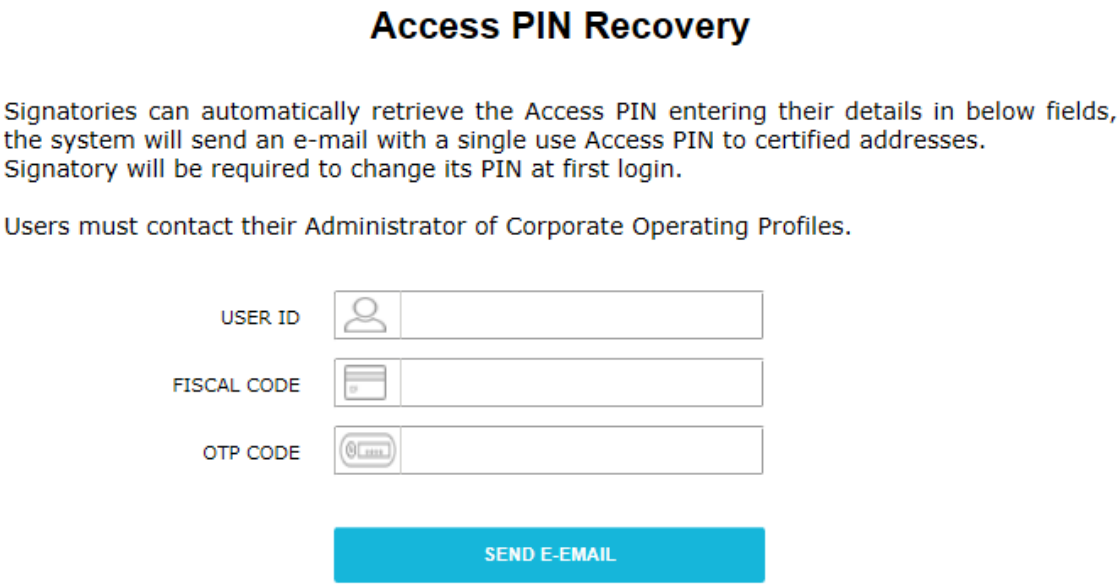


Warning: it is not possible to ask for this UserID recovery functionality if it has been asked an Access PIN recovery (see following chapters) and the single use PIN sent by the system has not been changed yet.

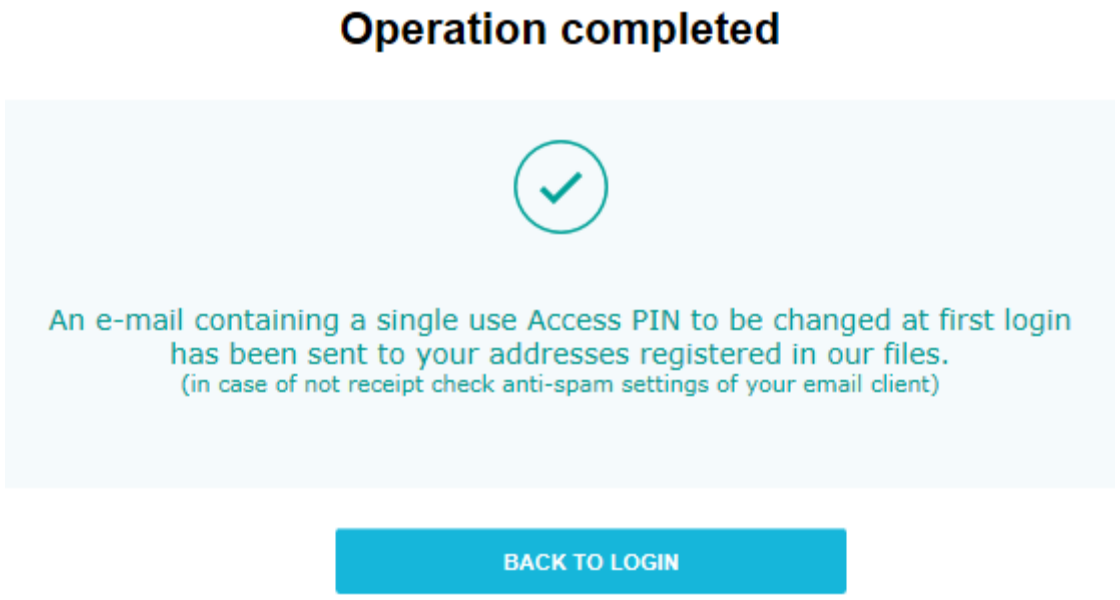
Users must require the userID recovery to their Administrator of the Company Operating Profiles.

4.2 Access PIN recovery *(signatories only)*

On UniWeb login page the signatories can ask the sending of their Access PIN (e.g. in case they forgot it) to the e-mail addresses registered for e-mail Alert service.
The link on the login page brings to the following page where the signatory must insert his/her userID and his/her fiscal code, confirming the request with an OTP.



The system proceeds to send a single use five digits Access PIN by e-mail to the e-mail addresses registered for e-mail Alert service for that signatory. The signatory is obliged to change the PIN at first login. The Access PIN recovery process resets the memory of the previous PINs, so it will not be controlled the rule that the chosen PIN must be different from the former three ones.

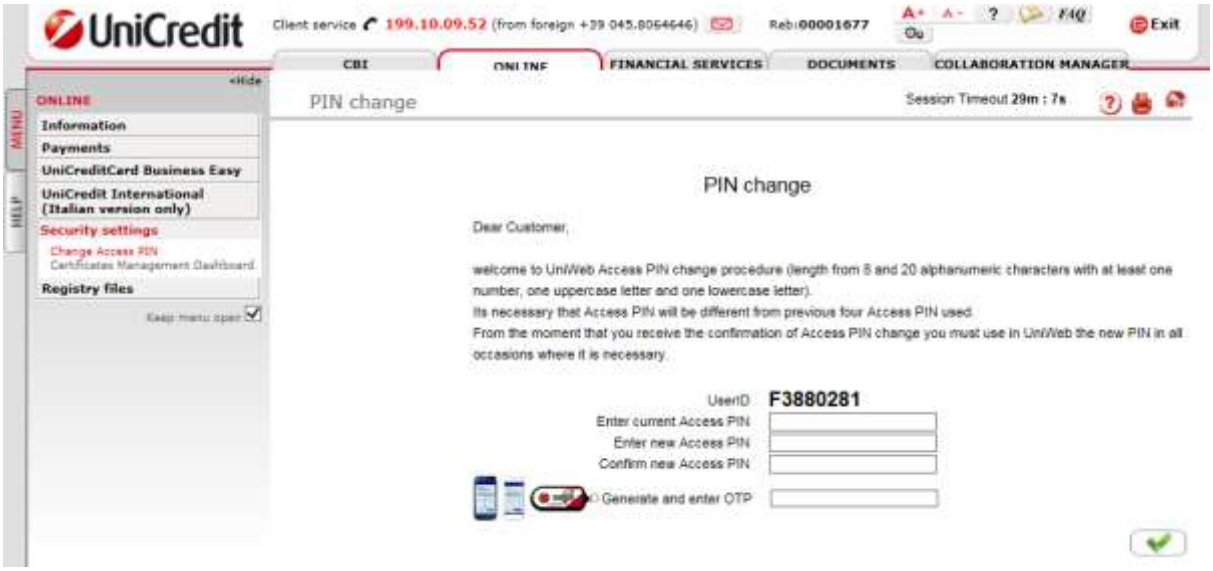


Warning: two consecutive requests of Access PIN recovery, without a login among the two, imply the lock of the user. To unlock it will be needed to contact the Bank.

Users must ask the Access PIN recovery to their Administrator of the Company Operating Profiles.

4.3 Access PIN change

Users can change their Access PIN when they want to, or when the system requires that (e.g. when Access PIN is expired).
The operation is done through the following page in the UniWeb's protected area in the section *ONLINE* > *Security Settings*, where users can see the userID assigned by the system and they must insert their actual valid (or expired) PIN and choose their new Access PIN, inserting it twice to avoid mistypings.



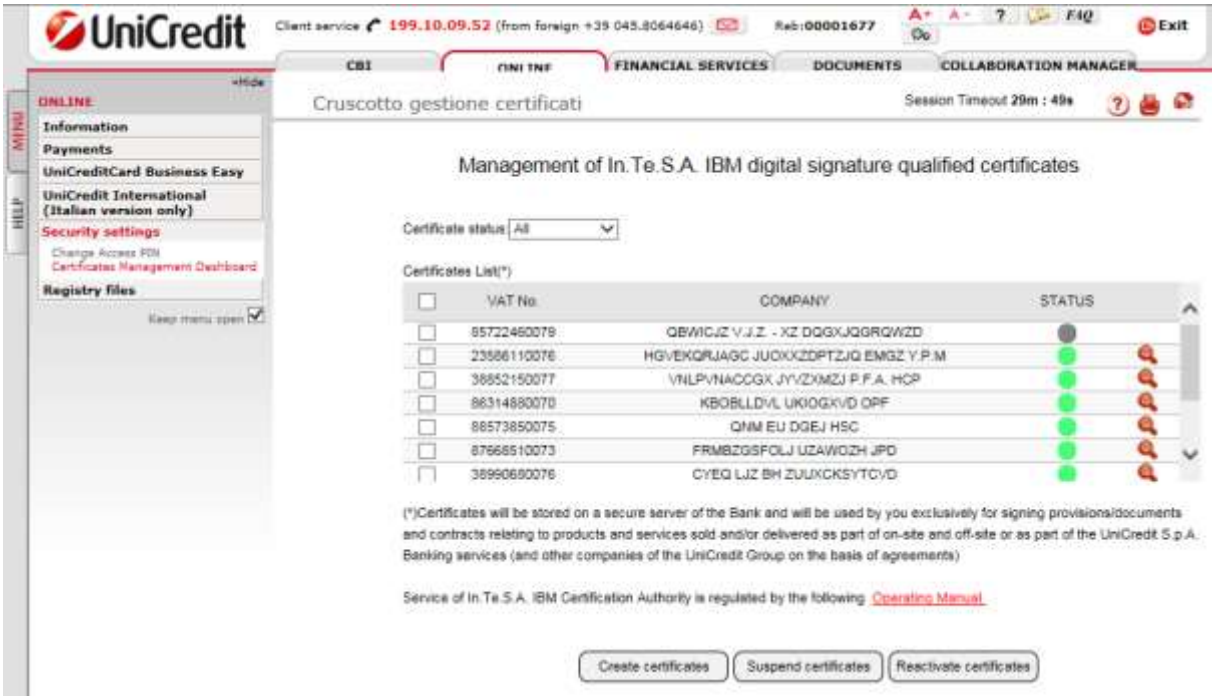
Access PIN must comply with following rules:

- From 8 to 20 alphanumeric characters (A-Z, a-z, 0-9)
- At least a number
- At least an uppercase letter
- At least a lowercase letter
- Different from last three formerly used by the signatory/user

Signatories must validate the inserted data with an OTP, while users must simply confirm it pressing the OK button.

4.4 Certificates Management Dashboard *(signatories only)*

Signatories can manage their signature qualified certificates on remote server through the following page in the UniWeb's protected area in the section *ONLINE* > *Security Settings*, where they can see all the certificates related to all the companies for which they are enabled to sign for the REB in use.

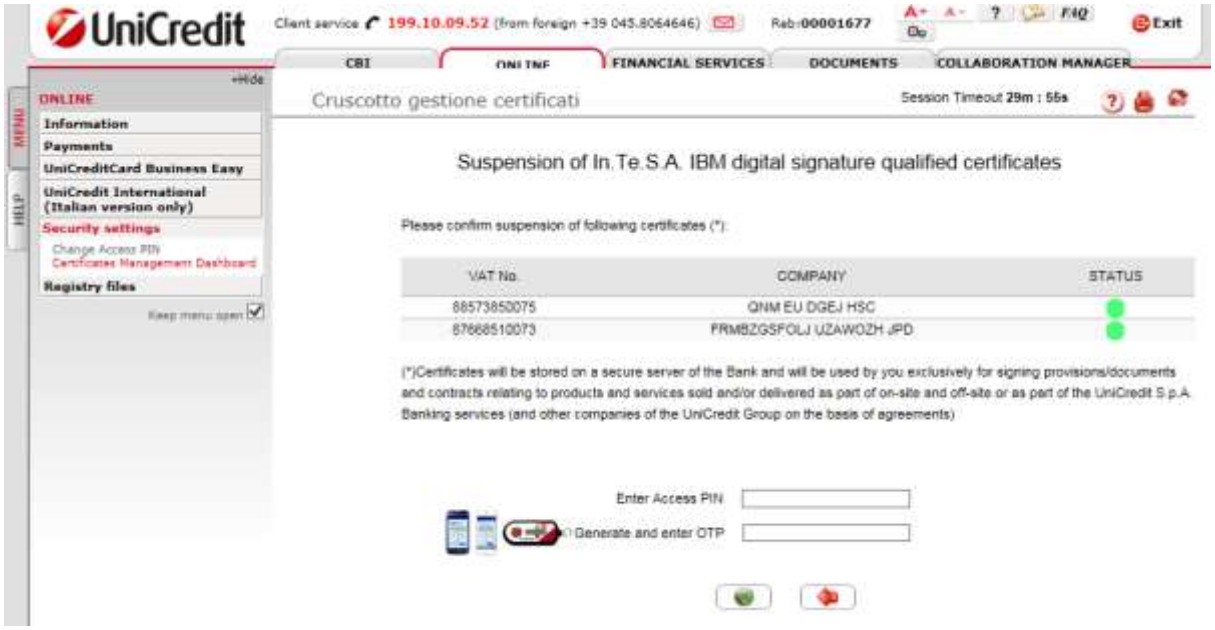


The available operations are:

- Cerfificates' creation
- Active certificates' suspension
- Suspended certificates' reactivation

Multiple operations (i.e. on more than one certificate with a single action) are allowed, provided that the selected certificates are in congruent statuses.

Once signatory selects certificates and chooses the desired operation, a summary page is displayed where signatory must confirm the request, inserting his/her Access PIN and an OTP to validate the operation (in the example it is shown the summary page for the suspension of two certificates).



If the desired operation is the creation of one or more certificates, then the signatory must also open the Certification Authority's Operating Manual link, and select the checkbox to confirm to have read it.

The system displays the progress of the operation (that potentially can involve many certificates) showing how many certificates have been created and how many are missing to end the process, showing at the end a confirmation message.

5 REB administration functionalities *(only Administrators of Company Operating Profiles)*

All the functionalities in ADMINISTRATION Tab becomes accessible only after inserting an OTP. The OTP is requested by the system only once for each working session when the Administrator tries to open an administration functionality, further accesses to that functionality or any other administration one during the working session will not imply a new request of an OTP.

5.1 Access PIN validity

The Administrators of Company Operating Profiles can define at a REB level the duration of the Access PIN for the users administered by them.
Such duration in UniWeb is set to 360 days by default, but if customers have more restrictive policies, then the Administrators of Company Operating Profiles can define a smaller limit (90, 180 or 270 days) through the following page in the UniWeb's protected area in the section *ADMINISTRATION* > *Security Settings*:

The click on Change button brings to the change page itself shown hereafter where the Administrator can choose the duration of the Access PIN for the users of the REB in use.

When the new duration is confirmed, then it has immediate effect on the following logins of the users of the REB.

5.2 **New user creation**

The Administrators of Company Operating Profiles can keep on creating users in the UniWeb's protected area in the section *ADMINISTRATION > Profile and parameters management*

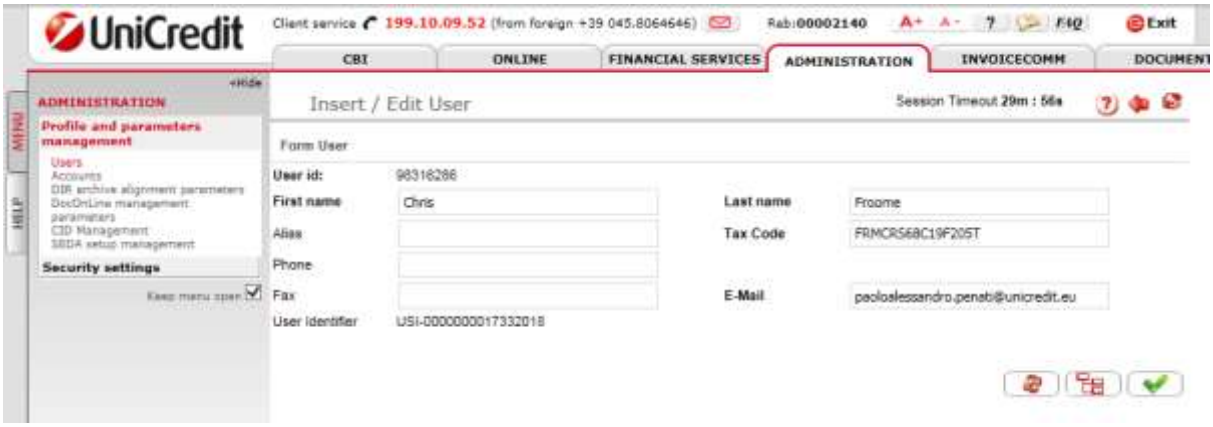
When a user is being created, then the system assigns to it an userID (to be remembered by the owner and that cannot be changed in the future) and the Administrator of Company Operating Profiles must choose a single use five digits Access PIN that must be inserted twice to avoid mistypings.

Both these credentials must be communicated to the owner (the user) who must use them for the first access (the user is forced by the system through the automatic PIN change procedure to change the single-use Access PIN, and to choose a new one at the first access).

Users can perform the UniWeb first access procedure immediately after their creation, but some functionalities (e.g. "Change Access PIN" menu) will be available only one day after their creation.

5.1 **User change – Access PIN Change**

The Administrators of Company Operating Profiles can keep on changing users' data in the UniWeb's protected area in the section *ADMINISTRATION > Profile and parameters management*.



If it is needed to recovery the Access PIN of the users (e.g. in case they forgot it), the Administrators of Company Operating Profiles can use the “Change Access PIN” button which opens a pop-up window where the Administrators of Company Operating Profiles can choose a new single use five digits Access PIN that must be inserted twice to avoid mistypings, and must be communicates to the user (the user is forced by the system to change the single-use Access PIN as for the first access).

The Access PIN recovery procedure for an user resets the memory of the previous PINs, so it will not be controlled the rule that the chosen PIN must be different from the former three ones.