UniWeb

Nuove credenziali di accesso e certificati qualificati di firma digitale su server remoto

Sommario

1 Presentazione del processo

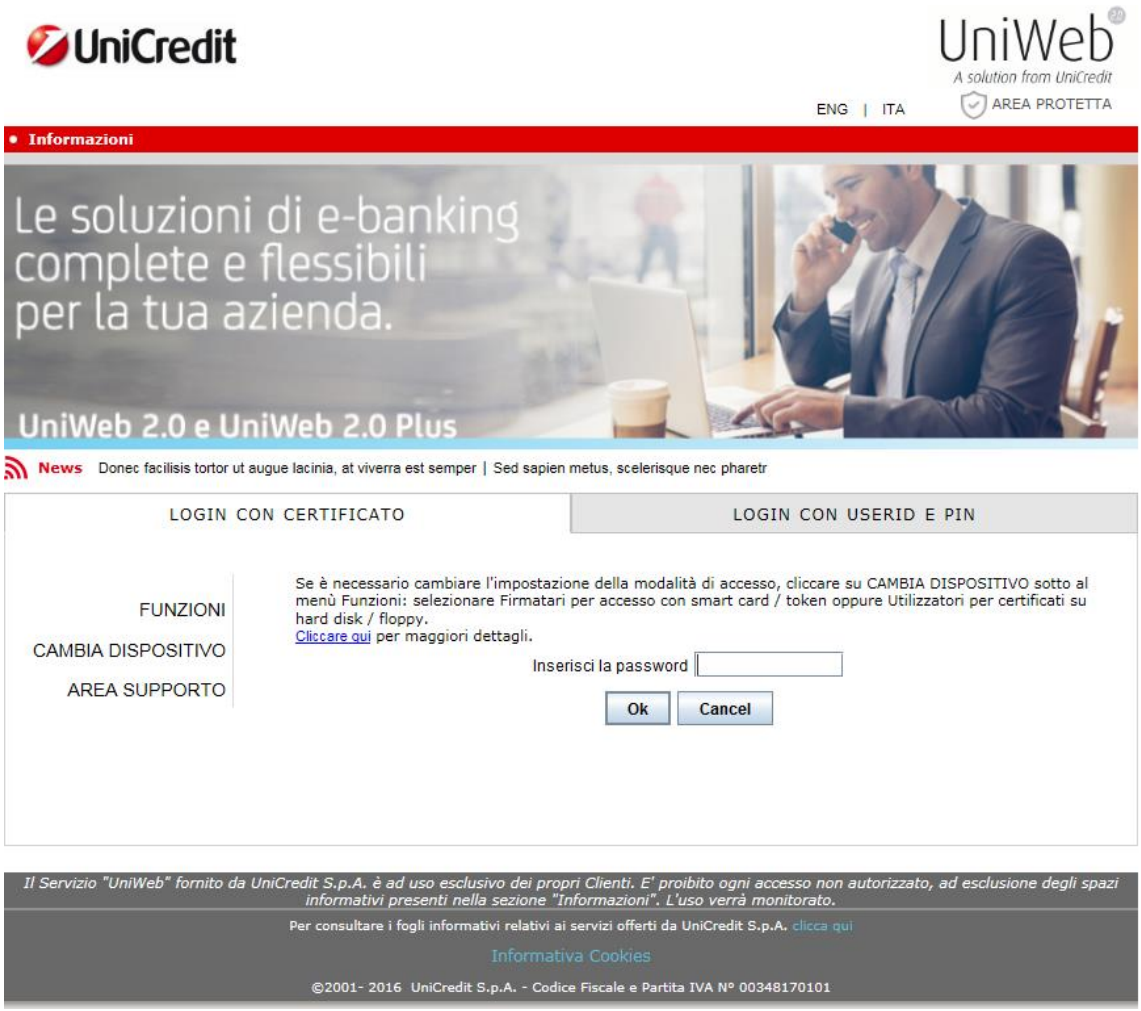
UniCredit, nell'evoluzione dei suoi prodotti di e-Banking destinati alla clientela aziendale, ha avviato una iniziativa di conversione delle utenze UniWeb esistenti.
L'intervento comporta l'eliminazione delle Applet Java nei processi di Login, Firma e Upload/Import, quindi non sarà più un requisito avere installato Java sulla macchina da cui ci si collega.

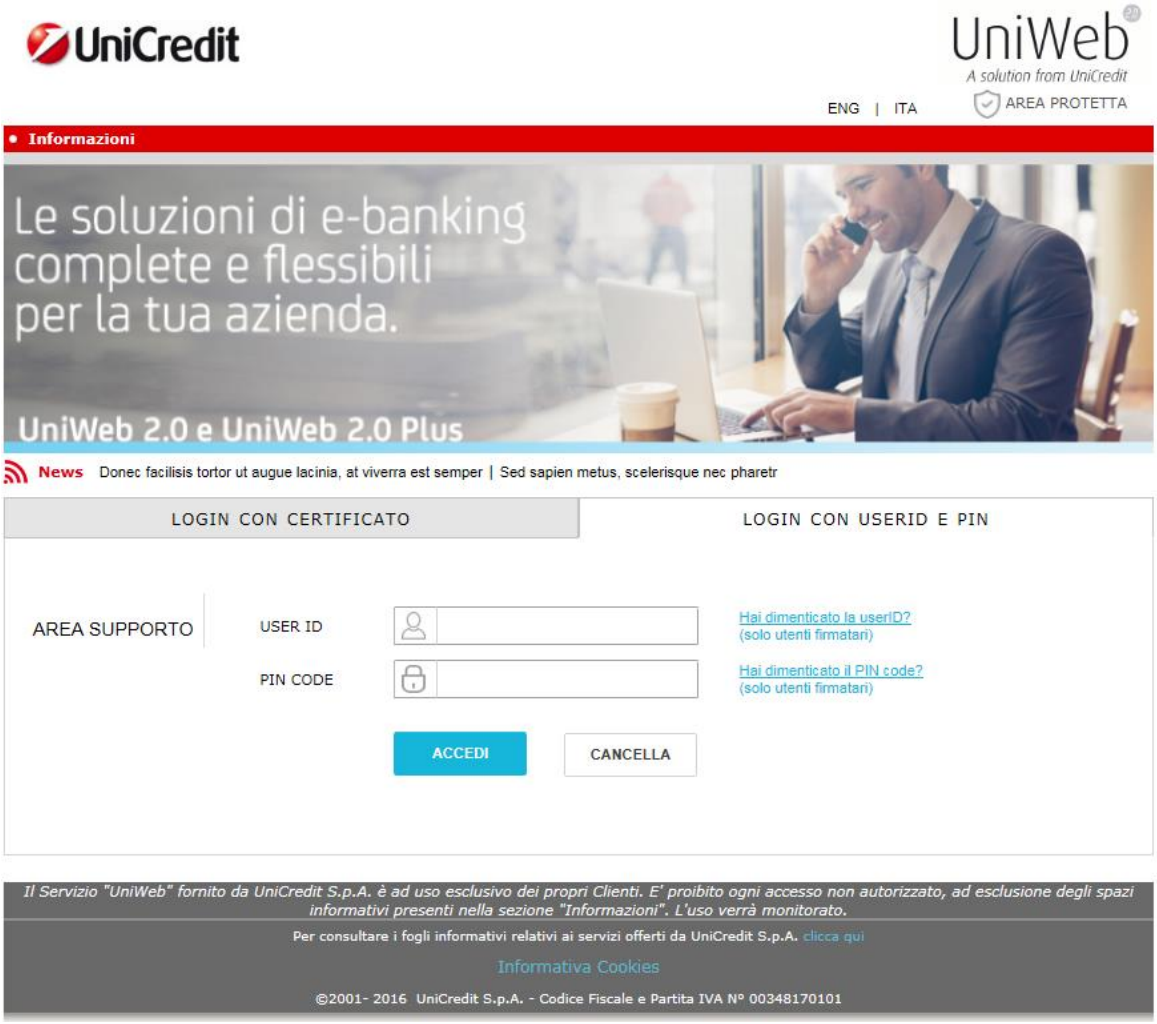
I procedimenti di Login e di Firma saranno semplificati e resi più efficienti, mentre l'Upload/Import conserverà l'aspetto e le funzionalità attuali.

Nella fattispecie dopo la migrazione od il censimento:

1. L'accesso degli utenti avverrà tramite l'inserimento di una userID, assegnata dal sistema durante il censimento o durante la migrazione, e di un PIN di Accesso scelto dal titolare dell'utenza al primo accesso (quando dovrà cambiare il PIN monouso ricevuto durante il censimento) o durante la migrazione
2. Per i firmatari la firma di qualsiasi disposizione / documento informatico avverrà tramite l'inserimento di una OTP (One Time Password) generata da uno dei dispositivi di sicurezza di cui ogni firmatario deve essere dotato. La firma sarà apposta attraverso un certificato qualificato di firma digitale su server remoto che sarà generato al primo accesso, durante la migrazione oppure nel corso della vita dell'utenza del firmatario, secondo le esigenze e le situazioni

La migrazione delle utenze esistenti avverrà progressivamente, quindi è previsto un periodo in cui coesisteranno utenze che accederanno e firmeranno secondo le vecchie regole e utenze già nel nuovo contesto.
Per consentire la coesistenza, la pagina di login è stata sdoppiata con due Tab corrispondenti alle due modalità di accesso, come illustrato nella seguente immagine.





Le utenze già dotate di userID e PIN di Accesso non potranno più accedere con la vecchia modalità di login o firmare con i vecchi certificati ossia la migrazione è irreversibile.
L'inserimento di 4 PIN di Accesso errati consecutivi porterà al blocco dell'utenza che potrà essere sbloccata in autonomia dai firmatari e ricorrendo al proprio Amministratori dei Profili Operativi Aziendali per gli utilizzatori.

2 Logiche di migrazione

2.1 Pre-requisiti

I prerequisiti per accedere alla procedura di migrazione sono i seguenti:

- Utilizzatori → essere dotati di credenziali di accesso valide
- Firmatari → essere dotati di credenziali di accesso valide e di un dispositivo di sicurezza generatore di OTP
- Amministratori dei Profili Operativi Aziendali → essere dotati di credenziali di accesso valide e di un dispositivo di sicurezza generatore di OTP

Gli ultimi due profili devono possedere un generatore di OTP per procedere alla migrazione, quindi è necessario che se ne dotino in tempo utile, qualora non già provveduto.

2.2 Calendario di migrazione

Gli utenti soggetti alla migrazione saranno suddivisi in “lotti” di migrazione per distribuirli nell’intervallo previsto per il procedimento (da Ottobre 2016 ad Aprile 2017), e la migrazione sarà proposta dal sistema agli utenti subito dopo il login una volta giunta la data di inizio del loro lotto.
Gli Amministratori dei Profili Operativi Aziendali riceveranno via e-mail una notifica con sette giorni di anticipo rispetto alla data di inizio del lotto di migrazione in cui sono inseritigli utenti (utilizzatori e firmatari) da loro amministrati.

Ciascun lotto avrà una durata indicativa di trenta giorni e gli utenti che non hanno ancora fatto la migrazione:

- Durante la durata del lotto: gli utenti dopo il login (e l’eventuale scelta REB per i firmatari multi REB) vedranno una pagina informativa che descriverà sommariamente il processo e permetterà di avviare immediatamente la migrazione (scelta consigliata) oppure di procedere in UniWeb posticipando ad altro momento la migrazione. La pagina è riportata di seguito

- Dopo la data di fine del lotto: gli utenti dopo il login (e l’eventuale scelta REB per i firmatari multi REB) vedranno la stessa pagina informativa precedente che permetterà solo di avviare immediatamente la migrazione. Non è più possibile accedere ad UniWeb senza migrare. La pagina è riportata di seguito

Procedura di migrazione

Gentile Cliente,

crei immediatamente le sue nuove credenziali di accesso ad UniWeb, passando alla nuova modalità di Login e di firma. Le sarà sufficiente memorizzare la userID assegnata dal sistema e scegliere il PIN di accesso.

Qualora lei sia Firmatario dovrà anche confermare, se non già fatto, i suoi recapiti (e-mail e numero di telefono mobile) e successivamente richiedere online e gratuitamente la generazione dei nuovi certificati di firma digitale su server remoto.

L'intero procedimento richiederà solo pochi minuti del suo tempo, proceda subito cliccando su Crea nuove credenziali.
Le ricordiamo che qualora non dovesse procedere in tempo utile non potrà più accedere ad UniWeb.

Se ha difficoltà a procedere la preghiamo di consultare la guida rapida o contattare il Contact Center al numero 199.100.952 (dall'estero +39 045.8064646).

Avvia migrazione

Per i soli firmatari sarà obbligatorio l'uso delle OTP per convalidare alcuni passaggi della migrazione; i firmatari che sono sprovvisti dopo il login vedranno una pagina informativa che gli notifica questa situazione e li invita a procurarsi un dispositivo di sicurezza tramite richiesta alla banca, lasciando loro solo la possibilità di proseguire.

Procedura di migrazione - dispositivo di sicurezza non trovato

Gentile firmatario,

per creare le sue nuove credenziali di accesso ad UniWeb, e passare alla nuova modalità di Login e di firma, è necessario che lei richieda un dispositivo di sicurezza generatore di One Time Password (OTP).
La invitiamo a procedere tempestivamente con la richiesta, online o contattando la sua Agenzia o il suo Gestore di riferimento.

Le ricordiamo inoltre che dopo 05 ottobre 2016 non potrà più procedere online e dovrà rivolgersi presso il suo Gestore o presso una Filiale, altrimenti non potrà più accedere ad UniWeb.

Se ha difficoltà a procedere la preghiamo di consultare la guida rapida o contattare il Contact Center al numero 199.100.952 (dall'estero +39 045.8064646).

Accedi ad UniWeb

La durata di un lotto di migrazione non implica che gli utenti debbano necessariamente migrare durante quel lotto, ma indica solo il periodo di facoltatività della migrazione.
Un utente (utilizzatore o firmatario) che dovesse accedere (con le logiche di login ante-migrazione) dopo la data di fine del suo lotto di migrazione, potrà comunque avviare la procedura di migrazione, ma non gli sarà possibile accedere ad UniWeb finché non si sarà dotato delle nuove credenziali (userID e Pin di Accesso).

2.3 Passi della migrazione

Il processo di migrazione prevede una serie di passi da compiere illustrati nei seguenti paragrafi. Fra parentesi è indicata la tipologia di utenti cui si riferiscono.
L'intero processo richiede pochi minuti una tantum per essere completato.

2.3.1 Certificazione e-mail (solo firmatari privi di e-mail Alert certificata)

Ai firmatari che non avessero almeno un indirizzo certificato per il servizio di e-mail Alert per il REB in uso viene chiesto di inserirne uno tramite la seguente pagina:

La certificazione della e-mail inserita avviene come di consueto tramite l'invio da parte di UniWeb di un codice numerico di verifica di cinque cifre alla e-mail inserita dall'utente.
Il firmatario deve inserire questo codice nella pagina seguente a conferma di avere l'accesso a quell'indirizzo e-mail e per evitare eventuali errori di battitura, convalidando l'operazione con una OTP.

UniCredit

UniWeb
A solution from UniCredit

Inserimento e certificazione e-mail

Firmatario

Nome ITUBSXHZ
Cognome PDWOLS
Email [redacted]

Per completare l'operazione inserire il codice che abbiamo inviato alla sua e-mail e confermare mediante OTP

Codice di attivazione


Genera ed inserisci una OTP

Conferma Indietro

Confermato

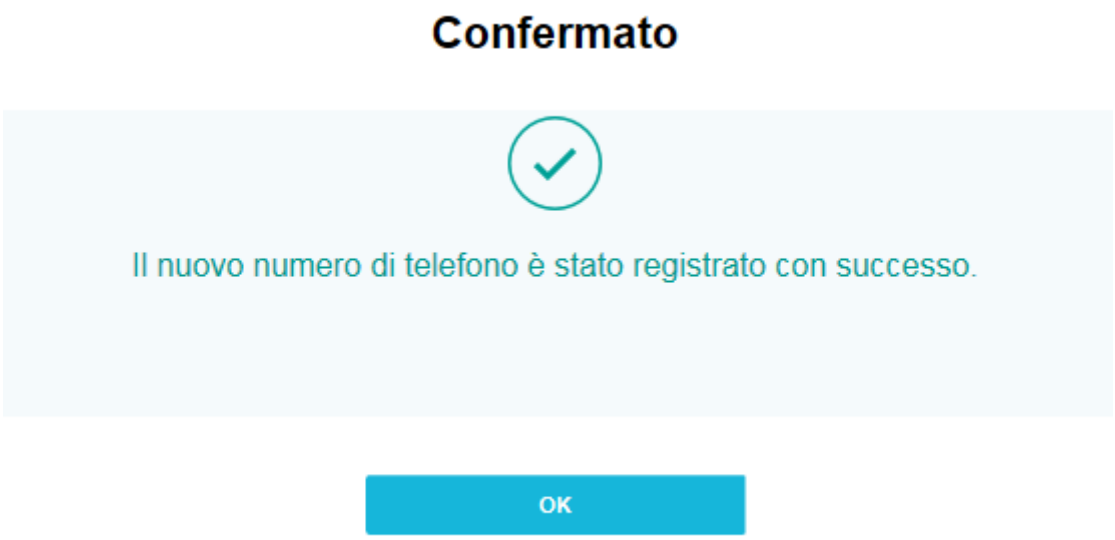
La nuova email è stata registrata.

OK

2.3.2 Certificazione numero di telefono mobile (solo firmatari privi di numero di telefono mobile certificato)

Ai firmatari che non avessero un numero di telefono mobile viene chiesto di inserirne uno tramite la seguente pagina:

La certificazione del numero di telefono mobile inserito avviene come di consueto tramite l'invio da parte di UniWeb di un codice numerico di verifica di cinque cifre via SMS al numero di telefono mobile inserito dall'utente.
Il firmatario deve inserire questo codice nella pagina seguente a conferma di avere l'accesso a quell'utenza telefonica e per evitare eventuali errori di battitura, convalidando l'operazione con una OTP.

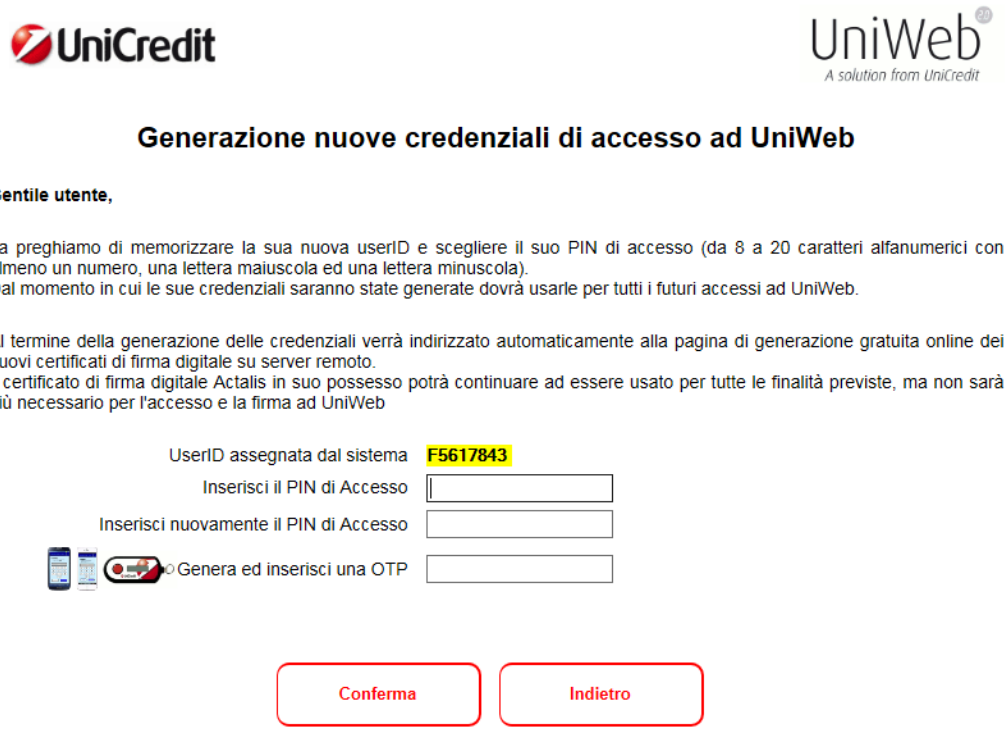


2.3.3 Censimento nuove credenziali di accesso

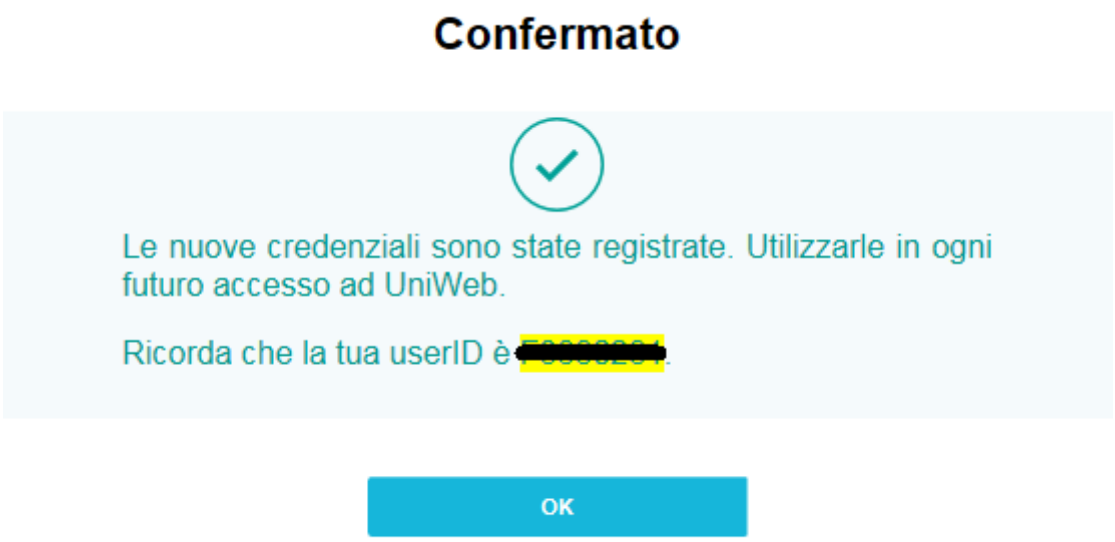
Agli utenti (utilizzatori e firmatari) viene presentata la seguente pagina nella quale trovano la userID che il sistema gli ha assegnato (da memorizzare e che non sarà modificabile in futuro) e devono scegliere il PIN di Accesso, inserendolo due volte per evitare eventuali errori di battitura. Il PIN di Accesso deve rispettare le seguenti regole:

- Da 8 a 20 caratteri alfanumerici (A-Z, a-z, 0-9)
- Almeno un numero
- Almeno una lettera maiuscola
- Almeno una lettera minuscola

I firmatari devono convalidare i dati inseriti con l'inserimento di una OTP, mentre gli utilizzatori devono semplicemente confermare l'operazione.
Di seguito la pagina di generazione delle nuove credenziali che viene presentata ai firmatari:



Dopo la conferma delle nuove credenziali gli utilizzatori possono proseguire in UniWeb, avendo terminato il processo di migrazione. Da quel momento le nuove credenziali devono essere utilizzate in ogni login all'applicazione.



Per i firmatari multi REB le credenziali sono valide per l'accesso a tutti i REB ai quali sono abilitati. I firmatari dopo la generazione delle nuove credenziali devono ancora generare (gratuitamente) i certificati qualificati di firma digitale su server remoto per tutte le società del REB in uso, processo descritto nel seguente paragrafo.
Qualora per un qualsiasi motivo la procedura di generazione dei certificati di firma non venga portata a termine, il firmatario ha comunque completato la generazione delle credenziali che da quel momento devono essere usate in ogni login all'applicazione.
Il processo non completato di generazione dei certificati di firma viene riproposto al successivo login su UniWeb.

2.3.4 **Generazione una tantum dei nuovi certificati qualificati di firma digitale su server remoto *(solo firmatari)***

Ai firmatari viene presentata la seguente pagina nella quale trovano la lista delle società per cui sono abilitati a firmare per il REB in uso:

UniCredit

UniWeb 3.0
A solution from UniCredit

Emissione certificati qualificati di firma digitale In.Te.S.A. IBM

Benvenuto alla procedura di generazione automatica e gratuita dei certificati qualificati di firma digitale su server remoto.

Sul Rapporto di Electronic Banking (REB) in uso sono state rilevate le sue abilitazioni a firmare per le seguenti aziende; verranno generati per lei i certificati necessari che verranno usati in occasione delle sue firme su UniWeb.
Le rammentiamo che è necessario dare il consenso alla generazione di tutti i certificati in elenco.

Consenso all'emmissione dei certificati(*)

☑	PARTITA IVA	AZIENDA
☑	23668990023	BMCK Y.E.Z.
☑	38990680076	CYEQ LJZ BH ZUUXCKSYTCVD
☑	87668510073	FRMBZGSFOLJ UZAWOZH JPD
☑	23586110076	HGVEKQRJAGC JUOXXZDPTZJQ EMGZ
☑	61762410019	I.I. GVL
☑	86314880070	KBOBLLDVL UKIOGXVD OPF

(*) I certificati saranno conservati su un server sicuro presso la Banca e saranno da lei utilizzabili esclusivamente per la sottoscrizione di disposizioni/documenti e contratti relativi a prodotti e servizi venduti e/o erogati nell'ambito dell'attività in sede e fuori sede ovvero nell'ambito di servizi di Internet Banking di UniCredit S.p.A. (e altre società del Gruppo UniCredit sulla base di accordi).

☑ Confermo di aver letto e compreso le regole del servizio offerto della Certification Authority In.Te.S.A. IBM di seguito riportate nel seguente Manuale Operativo. (è necessario aprire il link per confermare l'operazione).

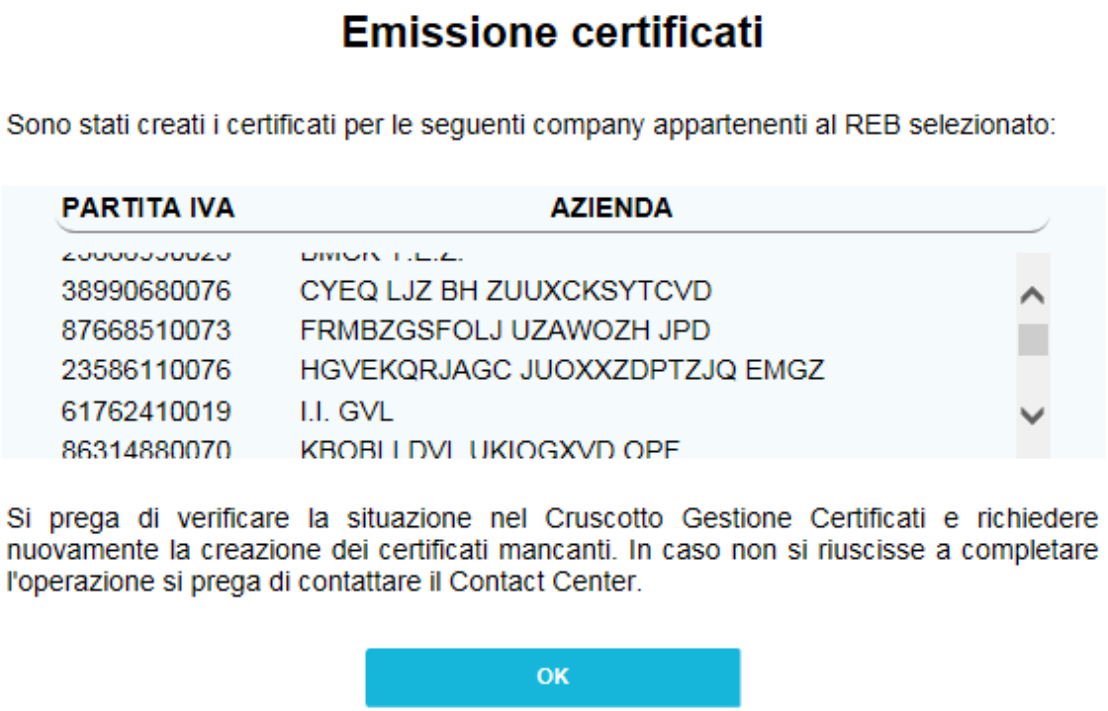
Inserisci il PIN di Accesso


Genera ed inserisci una OTP

Crea Certificati

Il firmatario per poter procedere deve selezionare tutte le società elencate, aprire il link al manuale operativo della Certification Authority e selezionare la casella che attesta la presa visione dello stesso, inserendo il proprio PIN di Accesso ed una OTP a convalida dell'operazione.

Una volta terminato il processo di emissione certificati, di cui viene mostrato l'avanzamento, la migrazione per quel REB è terminata ed il firmatario accede alla pagina iniziale di UniWeb potendo operare pienamente nel nuovo contesto.



Qualora il firmatario sia profilato per lavorare su più REB, al primo login su un altro REB (da effettuarsi con userID e PIN di Accesso) gli verrà presentata un'altra pagina di generazione una tantum dei certificati per le società per cui è abilitato a firmare per quel REB.

3 Primo accesso degli utenti censiti con userID e PIN di Accesso

Gli utenti già censiti con le nuove credenziali (userID e PIN di Accesso) devono svolgere alcune semplici operazioni di configurazione al primo accesso ad UniWeb, che potrà essere effettuato pochi minuti dopo il completamento del censimento da parte della Banca.
L'intero processo richiede pochi minuti una tantum per essere completato.

3.1 Modifica del PIN di Accesso monouso

Al censimento gli utenti sono dotati di un PIN di Accesso numerico di cinque cifre monouso (i firmatari l'hanno ricevuto dalla banca in busta PIN segreta, mentre gli utilizzatori l'hanno ricevuto dal proprio Amministratore dei Profili Operativi Aziendali).
Questo PIN va obbligatoriamente modificato al primo accesso tramite la seguente pagina, nella quale è visualizzata la userID che il sistema ha assegnato all'utente, il quale deve inserire il PIN monouso in suo possesso e scegliere il proprio nuovo PIN di Accesso, inserendolo due volte per scongiurare eventuali errori di battitura.

Il PIN di Accesso deve rispettare le seguenti regole:

- Da 8 a 20 caratteri alfanumerici (A-Z, a-z, 0-9)
- Almeno un numero
- Almeno una lettera maiuscola
- Almeno una lettera minuscola
- Differente dagli ultimi 3 precedentemente utilizzati dal firmatario/utilizzatore

I firmatari devono convalidare i dati inseriti con l'inserimento di una OTP, mentre gli utilizzatori devono semplicemente confermare l'operazione.

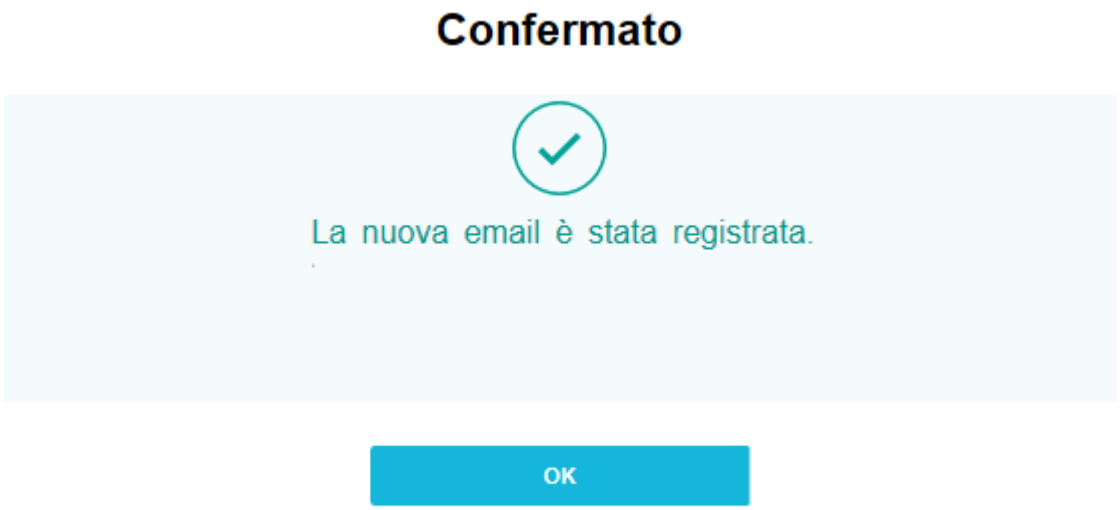
Dopo la conferma delle nuove credenziali gli utilizzatori possono proseguire in UniWeb, avendo terminato il processo di configurazione. Per i firmatari multi REB le credenziali sono valide per l'accesso a tutti i REB ai quali sono abilitati. Da quel momento le nuove credenziali devono essere utilizzate in ogni login all'applicazione.

I firmatari dopo la modifica del PIN di Accesso devono ancora fare alcuni passi di configurazione descritti nei seguenti paragrafi.
Qualora per un qualsiasi motivo i passi successivi non vengano portati a termine, il firmatario ha comunque completato la configurazione delle nuove credenziali che da quel momento devono essere usate in ogni login all'applicazione.
Le parti di processo non completate vengono riproposte al successivo login su UniWeb.

3.2 Certificazione e-mail

Ai firmatari viene chiesto di inserire un indirizzo certificato per il servizio di e-mail Alert per il REB in uso tramite la seguente pagina:

La certificazione della e-mail inserita avviene come di consueto tramite l'invio da parte di UniWeb di un codice numerico di verifica di cinque cifre alla e-mail inserita dall'utente.
Il firmatario deve inserire questo codice nella pagina seguente a conferma di avere l'accesso a quell'indirizzo e-mail e per evitare eventuali errori di battitura, convalidando l'operazione con una OTP.



3.3 Certificazione numero di telefono mobile

Ai firmatari viene chiesto di inserire un numero di telefono mobile tramite la seguente pagina:

La certificazione del numero di telefono mobile inserito avviene come di consueto tramite l'invio da parte di UniWeb di un codice numerico di verifica di cinque cifre via SMS al numero di telefono mobile inserito dall'utente.
Il firmatario deve inserire questo codice nella pagina seguente a conferma di avere l'accesso a quell'utenza telefonica e per evitare eventuali errori di battitura, convalidando l'operazione con una OTP.

3.4 Generazione una tantum dei nuovi certificati qualificati di firma digitale su server remoto

Ai firmatari viene presentata la seguente pagina nella quale trovano la lista delle società per cui sono abilitati a firmare per il REB in uso:

Il firmatario per poter procedere deve selezionare tutte le società elencate, aprire il link al manuale operativo della Certification Authority e selezionare la casella che attesta la presa visione dello stesso, inserendo il proprio PIN di Accesso ed una OTP a convalida dell'operazione.

Una volta terminato il processo di emissione certificati (il sistema mostra l'avanzamento indicando quanti certificati sono stati generati e quanti ne mancano) il sistema mostra un messaggio che conferma che la migrazione per quel REB è terminata ed il firmatario accede alla pagina iniziale di UniWeb, potendo operare pienamente nel nuovo contesto.

Qualora il firmatario sia profilato per lavorare su più REB, al primo login su un altro REB (da effettuarsi con userID e PIN di Accesso) gli verrà presentata un'altra pagina di generazione una tantum dei certificati per le società per cui è abilitato a firmare per quel REB.

4 Funzioni di amministrazione della propria utenza

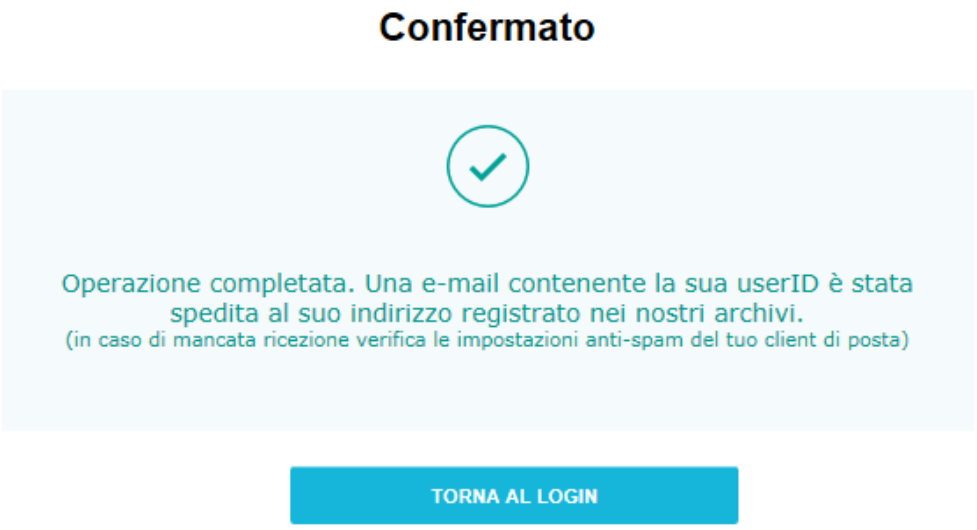
Gli utenti in possesso delle nuove credenziali (userID e PIN di Accesso) possono gestire credenziali e certificati qualificati di firma digitale su server remoto tramite alcune nuove funzioni di UniWeb.

Alcune funzioni, come indicato fra parentesi, sono limitate ai soli firmatari.

4.1 Recupero userID *(solo firmatari)*

Sulla pagina di login di UniWeb i firmatari possono chiedere l'invio della userID (ad esempio in caso di dimenticanza) presso gli indirizzi e-mail registrati per il servizio di e-mail Alert.
Il link presente sulla pagina di login porta alla seguente pagina dove il firmatario deve inserire il proprio codice fiscale, convalidando la richiesta con una OTP.

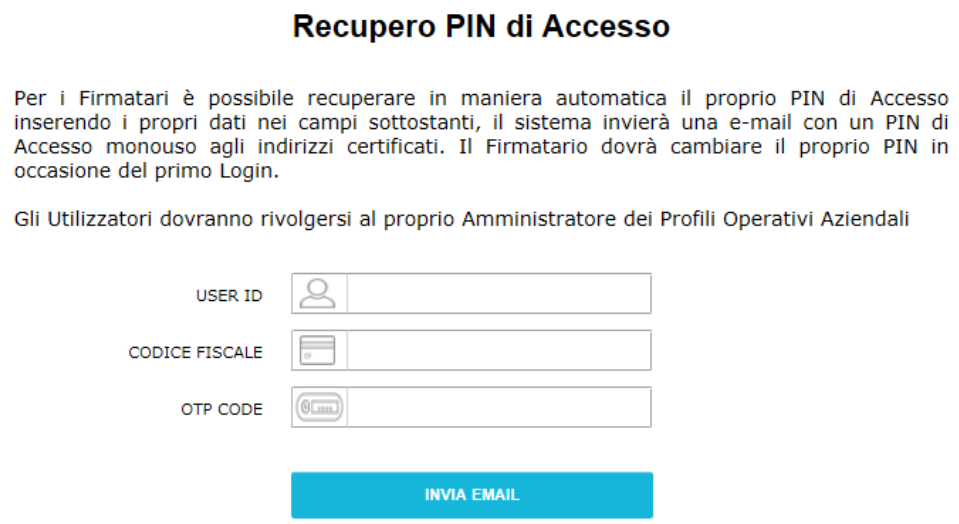
Il sistema provvede quindi ad inviare la userID per e-mail agli indirizzi di e-mail Alert registrati per il firmatario.



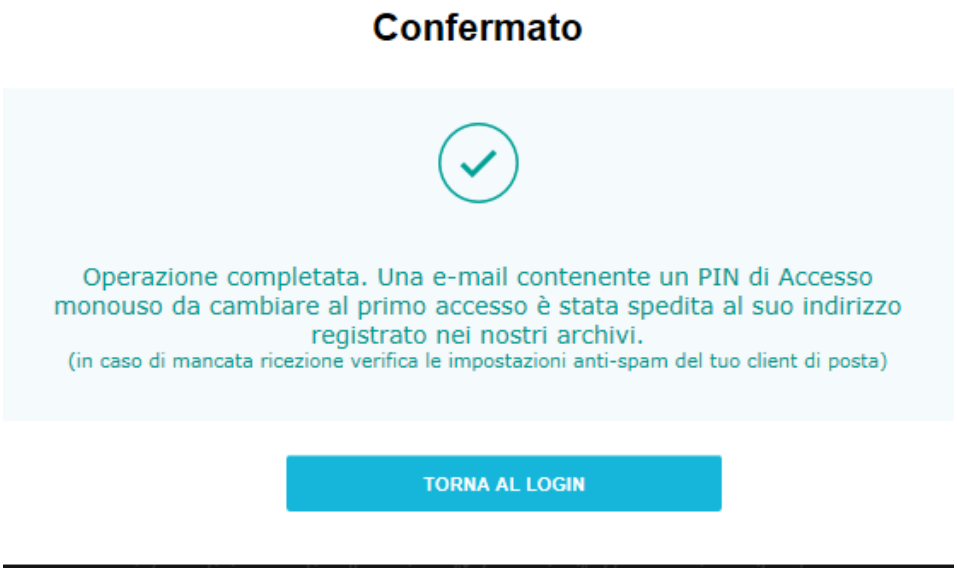
Attenzione: non è possibile richiedere questa funzione di Recupero UseerID se è stata richiesto un Recuperio PIN di Accesso (si veda i capitoli seguenti) e non è stato ancora modificato il PIN monouso inviato dal sistema.
Gli Utilizzatori devono invece rivolgersi al proprio Amministratore dei Profili Operativi Aziendali.

4.2 Recupero PIN di Accesso *(solo firmatari)*

Sulla pagina di login di UniWeb i firmatari possono chiedere l'invio del PIN di Accesso (ad esempio in caso di dimenticanza) presso gli indirizzi e-mail registrati per il servizio di e-mail Alert.
Il link presente sulla pagina di login porta alla seguente pagina dove il firmatario deve inserire la propria userID e il proprio codice fiscale, convalidando la richiesta con una OTP.



Il sistema provvede quindi ad inviare per e-mail agli indirizzi di e-mail Alert registrati per il firmatario un PIN di Accesso numerico monouso di cinque cifre. Il firmatario al primo accesso viene forzato a cambiare il PIN. La procedura di Recupero PIN di Accesso azzera la memoria dei PIN precedenti, pertanto non sarà più controllato il fatto che il PIN scelto sia differente dai tre precedenti.



Attenzione: due richieste consecutive di recupero del PIN di Accesso senza effettuare un accesso fra i due comporta il blocco dell'utenza. Per lo sblocco sarà necessario contattare la Banca.

Gli Utilizzatori devono invece rivolgersi al proprio Amministratore dei Profili Operativi Aziendali.

4.3 Modifica del PIN di Accesso

Gli utenti possono modificare il proprio PIN di Accesso quando lo desiderano o quando il sistema lo richiede (ad esempio quando il PIN di Accesso è scaduto).
L'operazione viene effettuata tramite la seguente pagina nell'area privata di UniWeb nella sezione *ONLINE* > *Impostazioni Sicurezza*, nella quale trovano la userID che il sistema gli ha assegnato e devono inserire il PIN in corso di validità (o scaduto) e scegliere il proprio nuovo PIN di Accesso, inserendolo due volte per scongiurare eventuali errori di battitura.

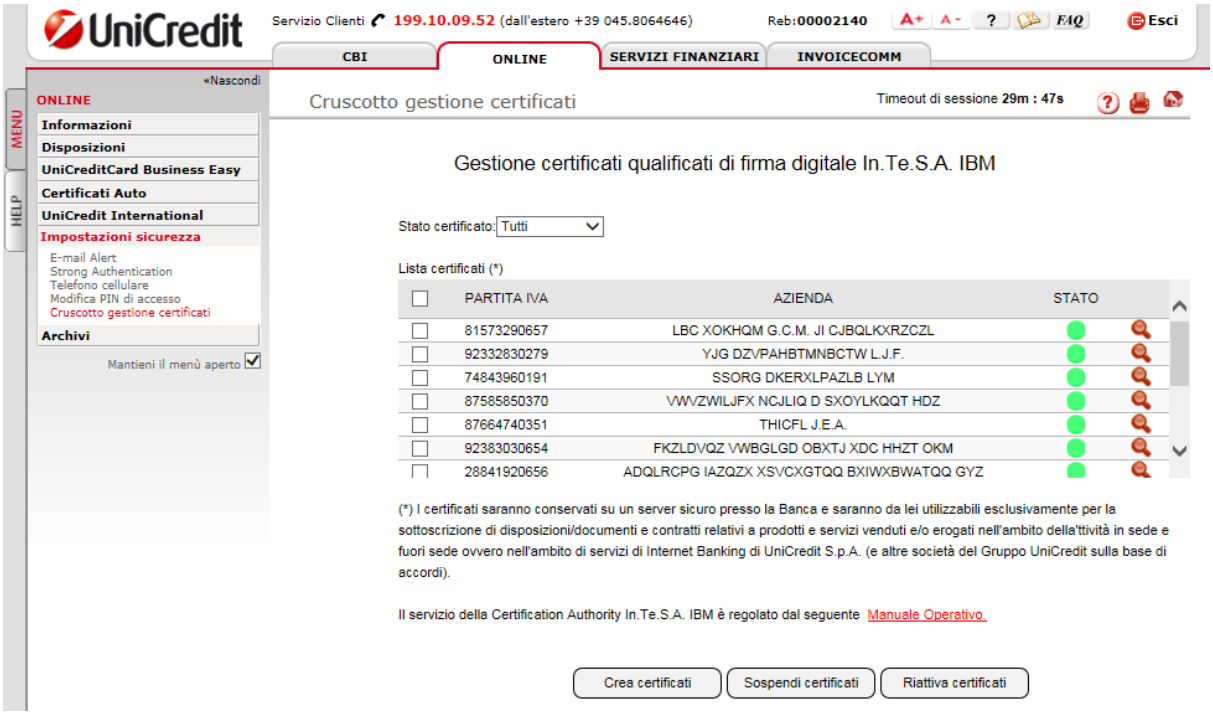
Il PIN di Accesso deve rispettare le seguenti regole:

- Da 8 a 20 caratteri alfanumerici (A-Z, a-z, 0-9)
- Almeno un numero
- Almeno una lettera maiuscola
- Almeno una lettera minuscola
- Differente dagli ultimi 3 precedentemente utilizzati dal firmatario/utilizzatore

I firmatari devono convalidare i dati inseriti con l'inserimento di una OTP, mentre gli utilizzatori devono semplicemente confermare l'operazione.

4.4 Cruscotto Gestione Certificati *(solo firmatari)*

I firmatari possono gestire i propri certificati qualificati di firma digitale su server remoto tramite la seguente pagina nell'area privata di UniWeb nella sezione *ONLINE* > *Impostazioni Sicurezza* dove possono visualizzare tutti i certificati relativi alle aziende per cui sono abilitati ad operare sul REB in uso.



Le operazioni ammesse sono:

- Generazione di certificati
- Sospensione di certificati attivi
- Riattivazione di certificati sospesi

Sono ammesse le operazioni multiple (ossia su più certificati contemporaneamente) a patto che i certificati coinvolti siano in stato congruente.

Una volta selezionati i certificati e scelta l'operazione che si vuole effettuare, viene presentata una pagina di riepilogo dove il firmatario deve confermare la richiesta inserendo il proprio PIN di Accesso ed una OTP a convalida (nell'esempio si è chiesta la sospensione di due certificati).

In caso di generazione di nuovi certificati prima di procedere alla conferma il firmatario deve aprire il link al manuale operativo della Certification Authority e selezionare la casella che attesta la presa visione dello stesso.

Il sistema mostra l'avanzamento dell'operazione (che potenzialmente potrebbe coinvolgere parecchi certificati) indicando quanti certificati sono stati generati e quanti ne mancano ed al termine presenta un messaggio di conferma.

5 Funzioni di amministrazione del REB *(solo Amministratori dei Profili Operativi Aziendali)*

Tutte le funzioni del Tab *AMMINISTRAZIONE* diventano accessibili solo previo inserimento di una OTP. L'OTP viene richiesta dal sistema una sola volta per sessione al primo tentativo di aprire una funzione di amministrazione, i successivi accessi alla stessa od a altre funzioni di amministrazione non comportano ulteriori richieste di OTP.

5.1 Durata del PIN di Accesso

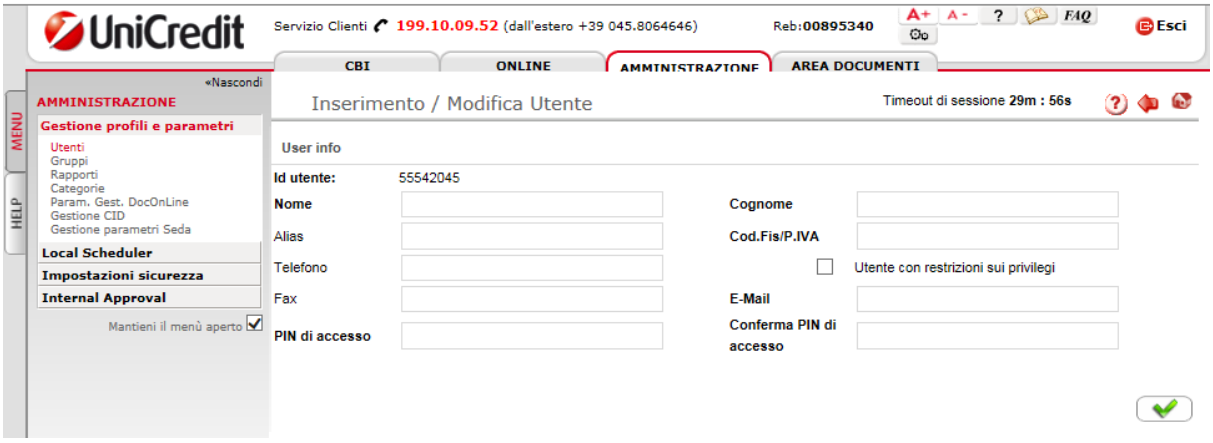
Gli Amministratori dei Profili Operativi Aziendali possono definire la durata del PIN di Accesso degli utenti da loro amministrati a livello di REB.
Tale durata è impostata per default a 360 giorni per UniWeb, ma in presenza di policy più restrittive gli Amministratori dei Profili Operativi Aziendali possono impostare un limite inferiore (90, 180 o 270 giorni) tramite la seguente pagina nell'area privata di UniWeb nella sezione *AMMINISTRAZIONE* > *Impostazioni Sicurezza*:

La pressione del tasto Modifica porta alla pagina di modifica vera e propria riportata di seguito sulla quale viene scelta l'effettiva durata del PIN di Accesso degli utenti del REB in uso.

In caso di conferma la modifica ha effetto immediato sui successivi Login degli utenti del REB.

5.2 **Creazione nuovo utilizzatore**

Gli Amministratori dei Profili Operativi Aziendali possono continuare a creare gli utilizzatori nell'area privata di UniWeb nella sezione *AMMINISTRAZIONE > Gestione Profili e Parametri*.



Alla creazione di questi utenti il sistema assegna una userID e l'Amministratore dei Profili Operativi Aziendali sceglie un PIN di Accesso numerico monouso di cinque cifre che deve essere inserito due volte per evitare errori di battitura.

Entrambe queste credenziali devono essere comunicate all'utilizzatore titolare che deve usarle per il primo accesso (l'utilizzatore è forzato a cambiare il PIN ricevuto ed a sceglierne uno nuovo al primo accesso tramite una procedura automatica proposta dal sistema).

Gli utilizzatori creati possono effettuare la procedura di primo accesso ad UniWeb immediatamente dopo la loro creazione, ma alcune funzionalità (es. menu "Modifica PIN di Accesso") saranno disponibili solo dalla giornata successiva alla creazione.

5.1 **Modifica utilizzatore – modifica PIN di Accesso**

Gli Amministratori dei Profili Operativi Aziendali possono continuare a modificare i dati degli utilizzatori firma nell'area privata di UniWeb nella sezione *AMMINISTRAZIONE > Gestione Profili e Parametri*.

Se è necessario cambiare il PIN di Accesso di un utilizzatore, l'Amministratore dei Profili Operativi Aziendali ha a disposizione un tasto "Cambio PIN di Accesso" che apre una finestra di pop-up dove l'Amministratore dei Profili Operativi Aziendali sceglie un PIN di Accesso numerico monouso di cinque cifre che deve comunicare all'utilizzatore che deve usarlo per il successivo accesso (l'utilizzatore è forzato a cambiare il PIN ricevuto ed a sceglierne uno nuovo come per il primo accesso).

La procedura di reset del PIN di Accesso di un utilizzatore azzera la memoria dei PIN precedenti, pertanto non sarà più controllato il fatto che il PIN scelto sia differente dai tre precedenti.