

Emissione Certificato Advanced Cloud Signature

User Experience

Marzo 2018

Aprire la pagina web store.intesigroup.com e selezionare il certificato di Advanced Cloud Signature come indicato dalla freccia

Scegli un prodotto

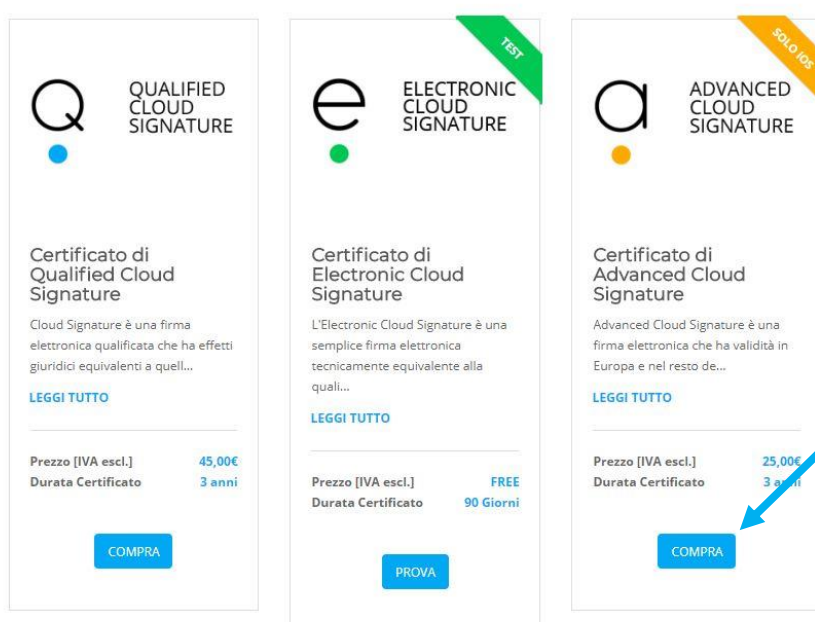


Fig. 1

Seguire passo passo le istruzioni dello Store compilando i campi richiesti. Al termine di questa procedura l'utente riceve un'e-mail con il link per avviare il processo di identificazione.

L'identificazione dell'utente è un passaggio chiave e obbligatorio, prima di procedere all'emissione del certificato digitale, che consentirà all'utente di firmare digitalmente i documenti.

Il processo di identificazione avviene tramite un'App mobile sviluppata da Intesi Group: **IDentify** (attualmente disponibile solo in versione iOS). L'App raccoglie un set di informazioni relative all'utente e le foto dei documenti identificativi che successivamente vengono inviate in modo sicuro al RAO (Registration Authority Officer) per la verifica e successiva approvazione.

Il vantaggio di IDentify consiste nel fatto che l'utente può completare la procedura di identificazione a sua discrezione, compilando le informazioni richieste in momenti diversi, anche offline, decidendo autonomamente quando inviare il set di informazioni al RAO.

L'App IDentify può essere utilizzata per supportare il processo di identificazione di diversi utenti (ognuno di essi avrà ovviamente accesso con le proprie credenziali). È necessario quindi un solo iPhone/iPad per gestire il processo di tutti gli utenti, se non tutti dispongono di device iOS.

Il RAO verifica che tutte le informazioni fornite dall'utente siano complete e coerenti. Successivamente invia sia a) una notifica push a IDentify che b) una e-mail all'utente relativa al completamento del processo di registrazione (vedere Fig. 2).

Se qualcosa va storto in fase di verifica (ad esempio, mancata corrispondenza delle informazioni fornite, foto poco chiare, etc. ..) la notifica riporterà gli errori all'utente, a cui verrà quindi richiesto di correggere e inviare nuovamente il set di informazioni di identificazione.

Tipicamente il processo di identificazione viene completato con una singola interazione "virtuale" tra l'utente e il RAO.

Il prossimo step è la registrazione e l'emissione del certificato di firma

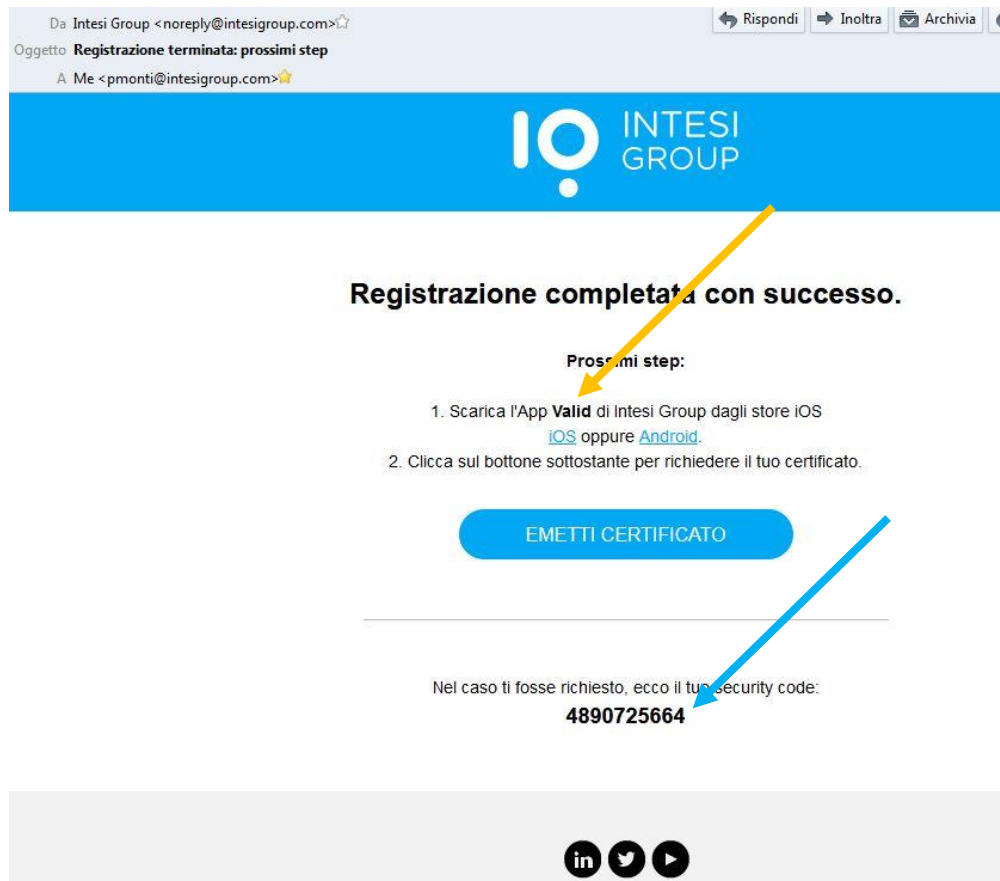


Fig. 2

Per procedere con questa fase, bisogna aprire la mail da smartphone e selezionare il collegamento (iOS o Android, vedere freccia gialla in Fig. 2) per scaricare l'App **Valid**. L'App servirà per la fase di emissione del certificato e fornirà (successivamente) l'OTP (One Time Password - password temporanea) richiesta durante la fase di firma.

Dopo il download, eseguire la login all'App.

- Utente = indirizzo e-mail fornito durante la fase di acquisto
- Password = password selezionata durante la fase di acquisto

L'utente dovrà quindi accedere al portale Time4Mind a questo indirizzo:

<https://www.time4mind.com/homepage.php>

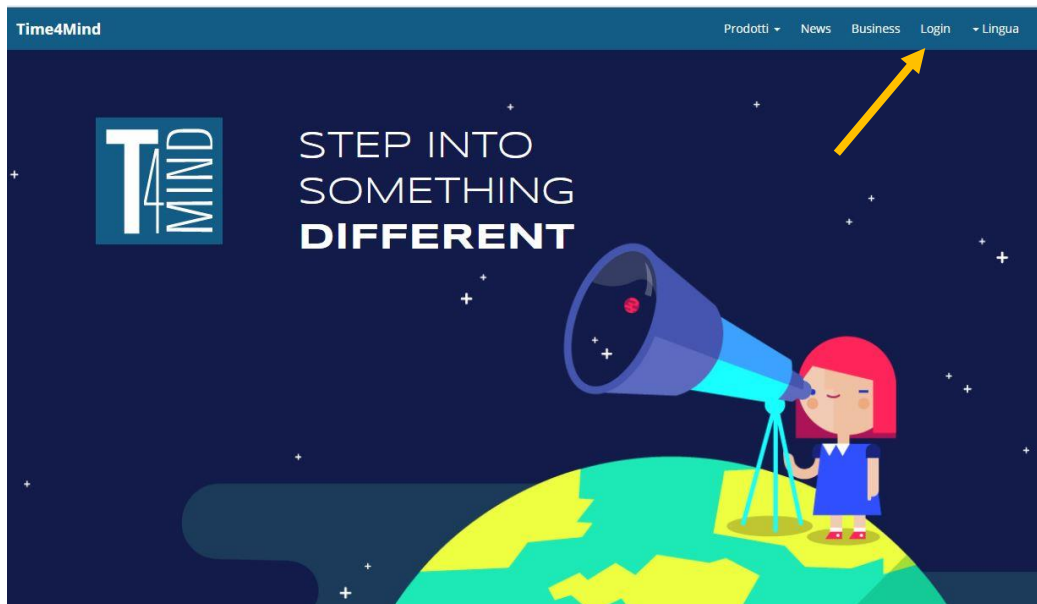


Fig. 3

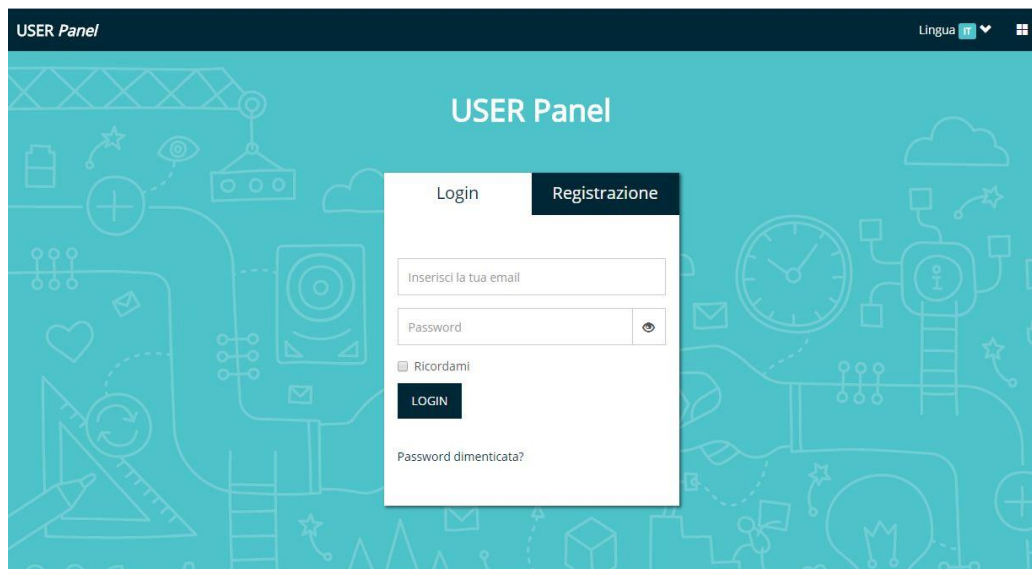


Fig. 4

Eseguire la login fornendo:

- Utente = indirizzo e-mail fornito durante la fase di acquisto
- Password = password selezionata durante la fase di acquisto

Completata la login selezionare la funzione Emissione Certificato presente sulla sinistra dello schermo.

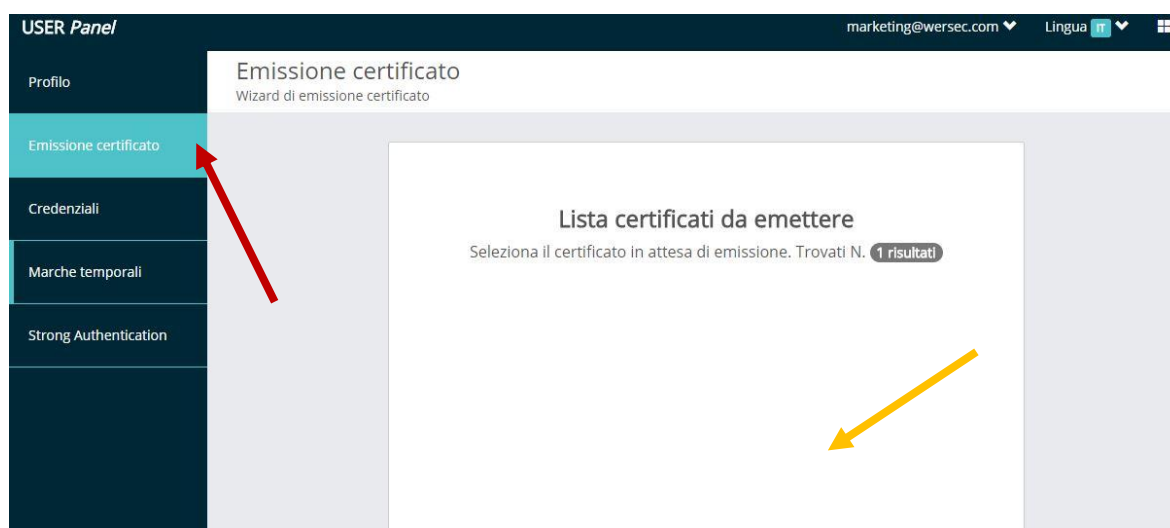


Fig. 5

Inserire il codice di sicurezza ricevuto nell'e-mail (vedere Fig. 2); il campo verrà automaticamente visualizzato nell'area identificata dalla freccia gialla.

L'utente riceverà una notifica push nell'App Valid e dovrà confermare l'emissione del certificato.

Con questo passaggio si completa la procedura di emissione del certificato di firma digitale (Advanced Cloud Signature).

Per completezza l'utente riceve anche una mail di conferma come visibile in Fig. 6.

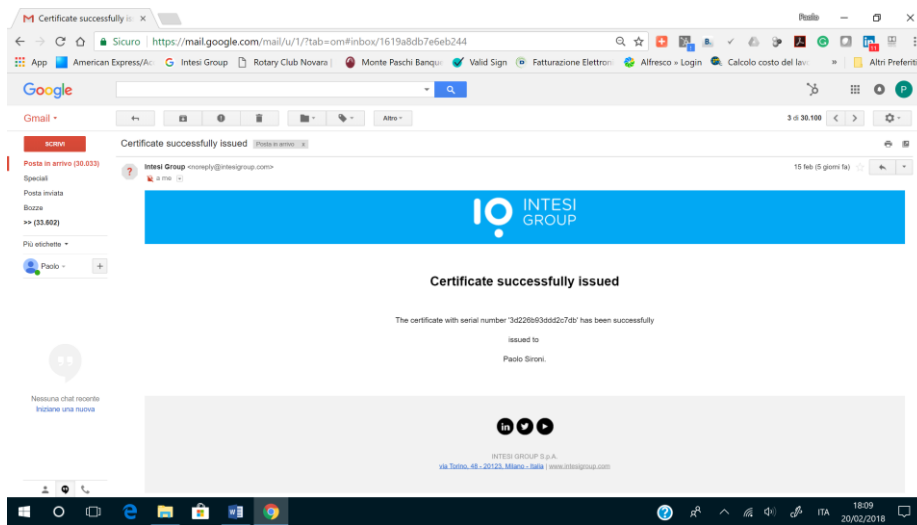


Fig. 6