

Token migration via Time4Mind portal - Android

Quick user guide

November 2020

History

Document	Version	Date	Author	Approval
Guida utente	1.0	12/05/2020	S. Blanchetti	P. Monti
	1.1	10/6/2020	P. Sironi	P. Monti
	1.2	16/09/2020	S. Blanchetti	P. Monti
	1.3	05/10/2020	S. Blanchetti	P. Monti

Token migration via Time4Mind portal user guide

This guide describes the process of transferring an authentication token from one mobile device to another. This operation is necessary in case of device replacement and also when the App is deleted and then reinstalled on the same device.

The authentication token is used every time you digitally sign in order to certify your identity.

The authentication token is uniquely linked to the digital signature certificate. In the event that a customer has multiple certificates, even of different types (e.g. a qualified certificate - Qualified Cloud signature - and an advanced certificate - Advanced Cloud signature), there will be as many tokens as there are certificates associated with the same customer.

For security reasons, the token can be active and usable on only one mobile device (smartphone or tablet) at a time.

To start the token transfer process, you must connect to the "User Portal" portal (<https://user.time4mind.com/secure/credentials.php>) and enter your credentials (email address and password).

If the password is forgotten, it is possible to carry out the recovery procedure by clicking "Forgot password?".

Once logged in to the "User Portal" reserved area, click the tab from the left menu "Strong Authentication" (Point 1).

Then select "Transfer" (Point 2):

The screenshot shows the 'User Portal' interface for 'Strong Authentication'. The left sidebar contains navigation options: Profile, Certificate Issuance, Certificates, Identifications, Timestamps, Strong Authentication (highlighted with a red box and arrow labeled '1'), and OTSP Documents. The main content area is titled 'Strong Authentication' and includes a sub-header 'Manage Strong Authentication services'. Below this are two service entries, each with a 'MIGRATE' button highlighted by a red box and arrow labeled '2'. The first entry is for a service with ID 205831 on a Samsung SM-G970F device. The second entry is for a service with ID 204021 on a Phone12.3 device. A 'Connected Certificate(s)' section shows one certificate.

You'll be asked to enter a One Time Password (OTP) to start the transfer operation will open. To get the OTP, click "**Request OTP via email**".

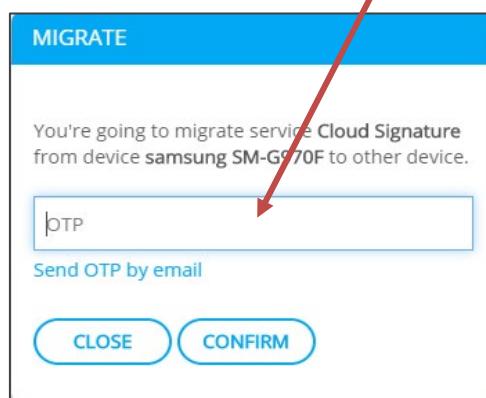
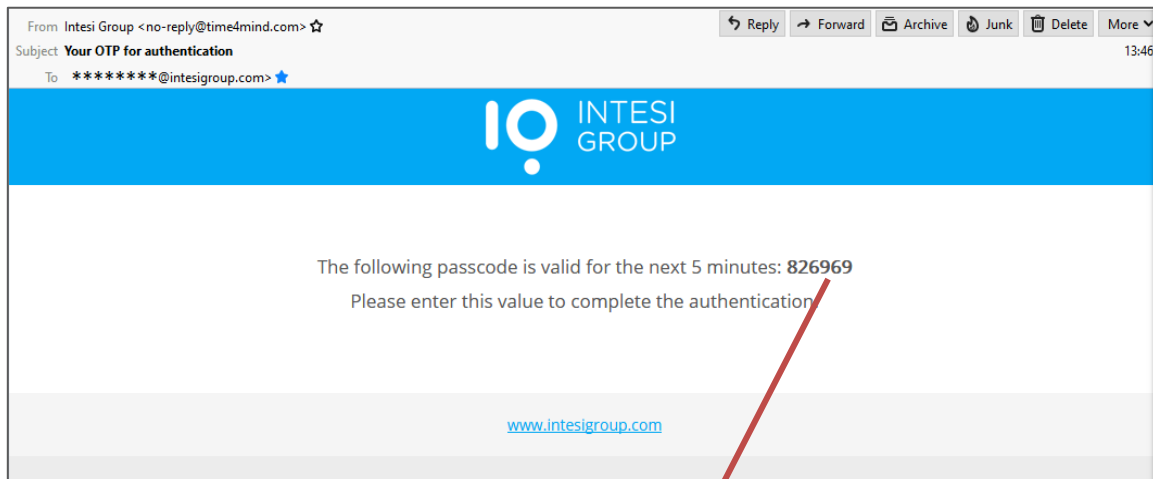
MIGRATE

You're going to migrate service **Cloud Signature** from device **samsung SM-G970F** to other device.

[Send OTP by email](#)

[CLOSE](#) [CONFIRM](#)

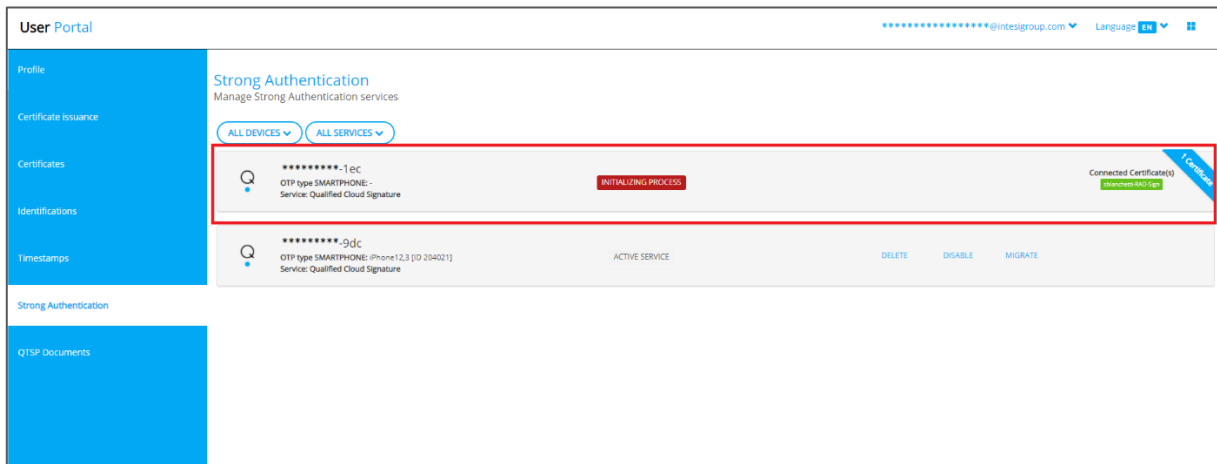
An e-mail will be sent immediately to the address you used for registration on the Time4Mind portal.



The 'MIGRATE' dialog box contains the following text: 'You're going to migrate service Cloud Signature from device samsung SM-G970F to other device.' Below this is an input field containing '0TP'. A red arrow points from the passcode '826969' in the email above to this input field. Below the input field is a link 'Send OTP by email' and two buttons: 'CLOSE' and 'CONFIRM'.

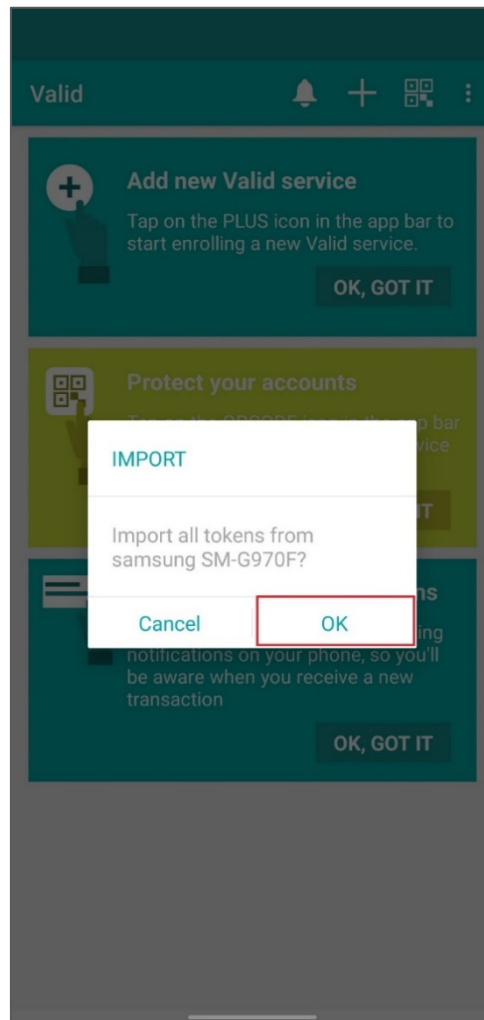
Take note of the received OTP (123456 is purely an example) by email and enter this value in the "TRANSFER" screen, then click "CONFIRM".

In the "Strong Authentication" view, the token will look like this:



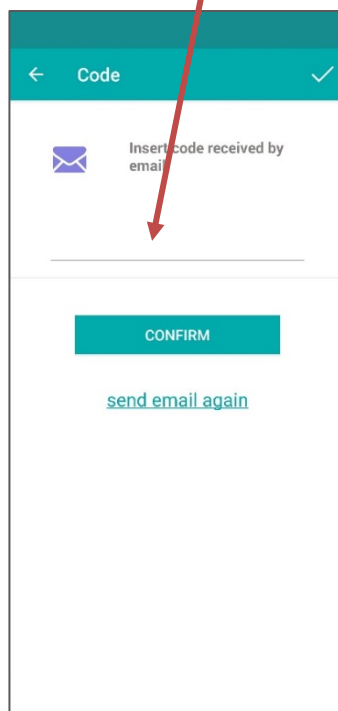
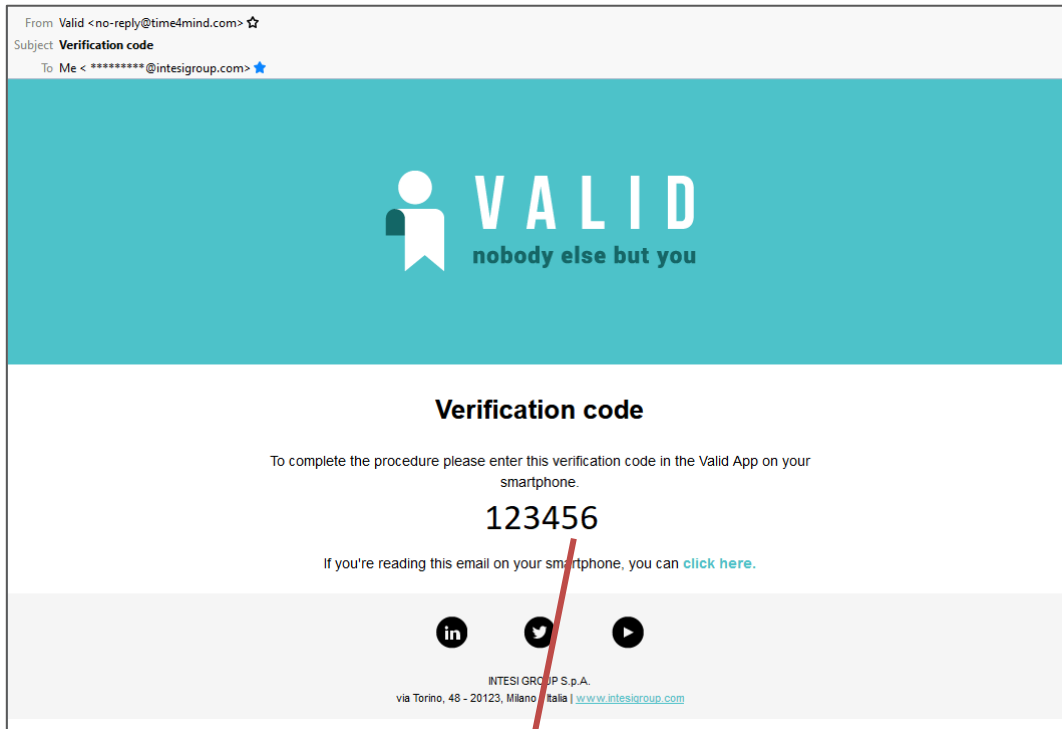
Now you can install the App on the new device or proceed with the uninstallation-installation from the App from the same device.

At the first access to the App, if pre-existing tokens are found on the device (in case of an uninstallation - installation of the App), the following message will be displayed:

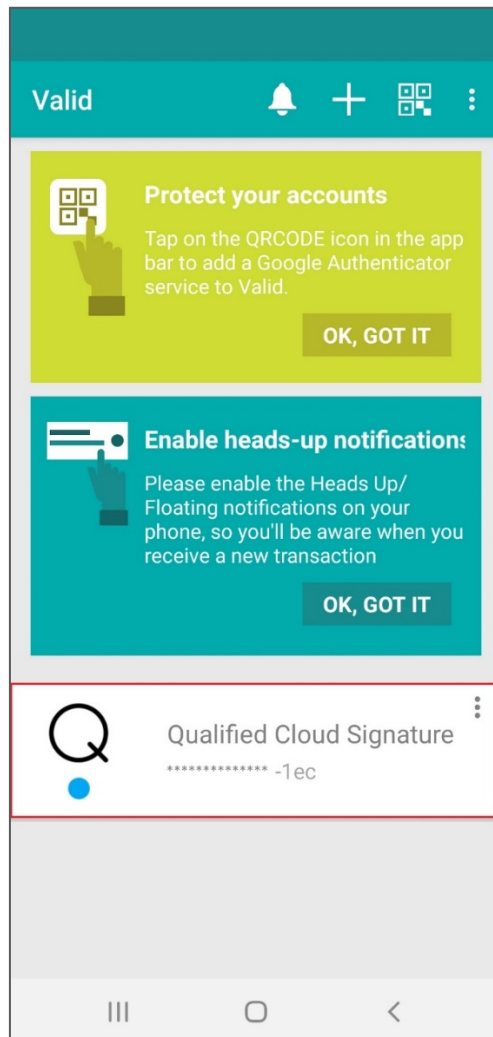


By selecting "OK" you will be asked to enter the OTP code received via email to finish the procedure:

The OTP code received in the following email must be inserted into the app:

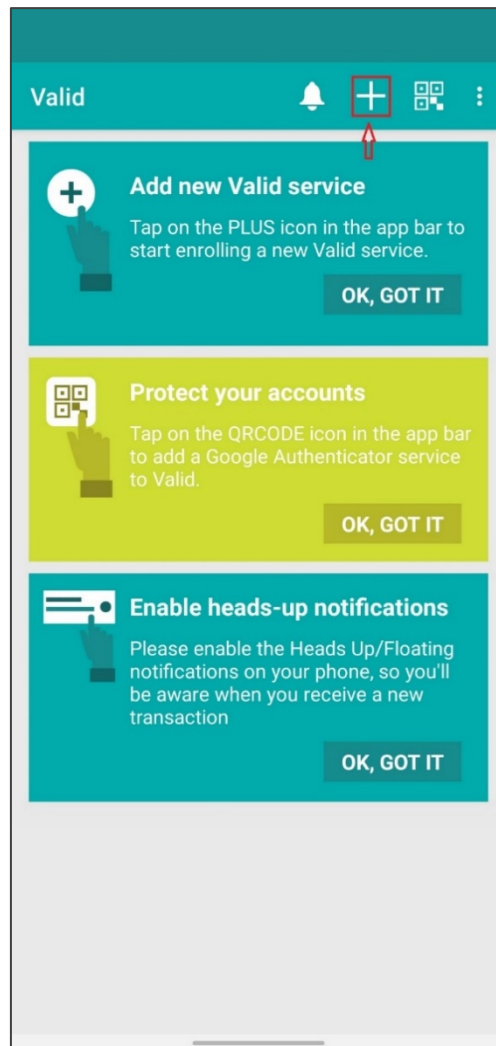


Once the OTP is inserted, the tokens on the device will be reloaded in the app:

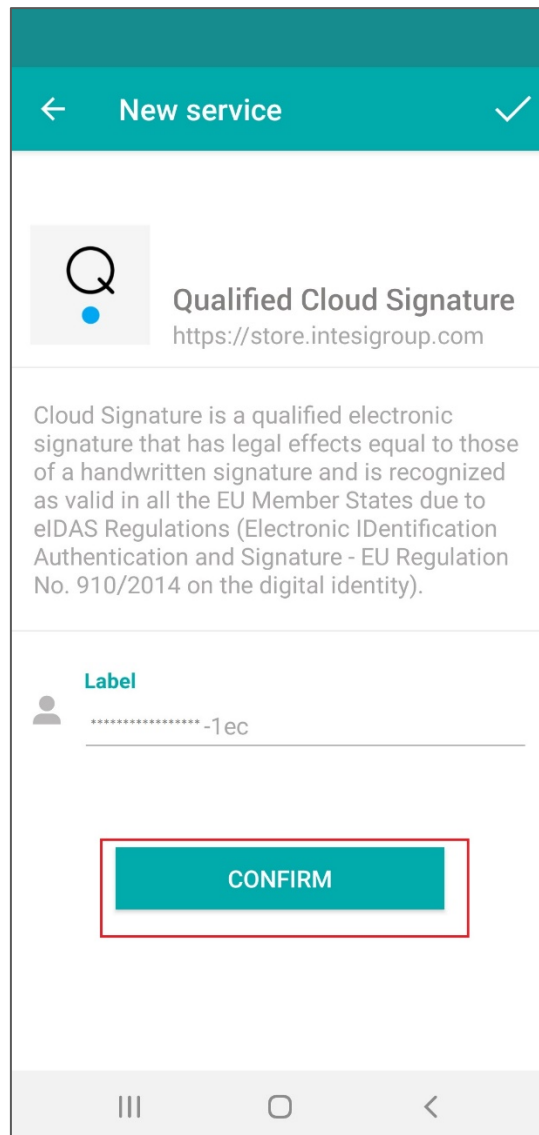


In the case of a new device, there will be no new tokens to be imported, or there may be tokens that have been activated directly and only on the new device.

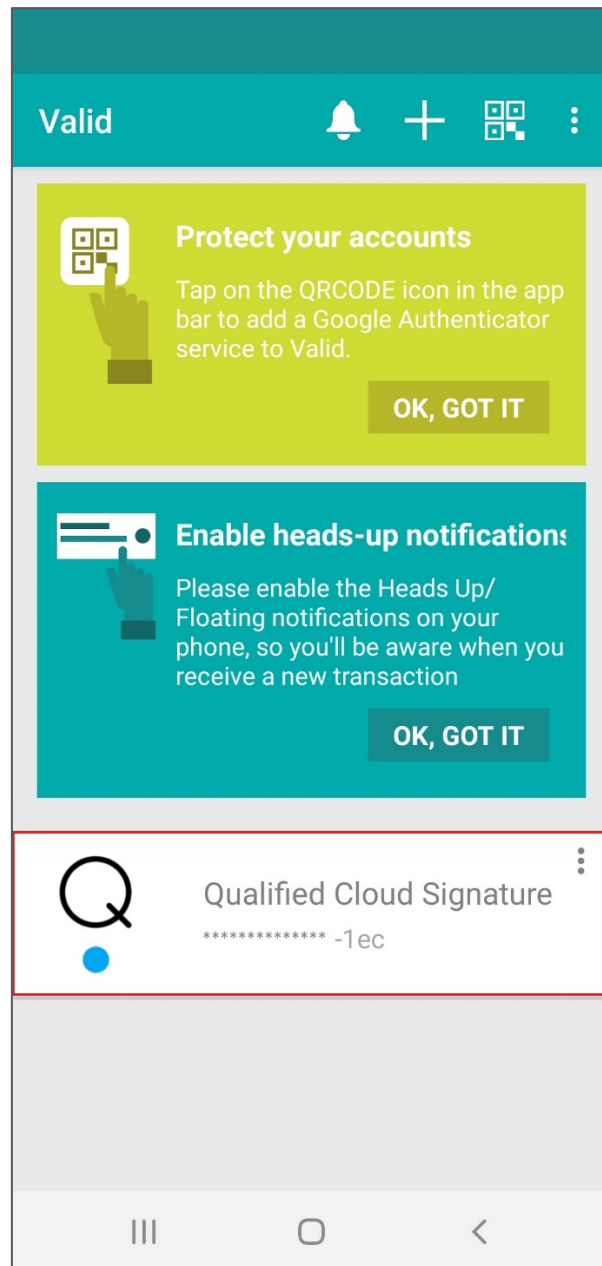
Then click on the "+" in the upper right corner of the screen.



The following view will be loaded. Just select "Confirm":



After selecting "Confirm", the token will be associated with the App:



The Time4Mind portal will be updated with the association of the new device with the token:

The screenshot shows the 'User Portal' interface for 'Strong Authentication'. The page title is 'Strong Authentication' with the subtitle 'Manage Strong Authentication services'. There are two tabs: 'ALL DEVICES' and 'ALL SERVICES'. A table lists two active services. The first row is highlighted with a red border and includes a 'Connected Certificate(s)' button and a 'Configure' badge. The second row has 'DELETE', 'DISABLE', and 'MIGRATE' buttons.

ID	Device Information	Status	Actions	Additional Info
*****-1ec	OTP type SMARTPHONE: samsung SM-G970F [ID 205831] Service: Qualified Cloud Signature	ACTIVE SERVICE	DISABLE MIGRATE	Connected Certificate(s) *****@*****.com
*****-9dc	OTP type SMARTPHONE: iPhone12,3 [ID 204021] Service: Qualified Cloud Signature	ACTIVE SERVICE	DELETE DISABLE MIGRATE	