HOW TO DETERMINE IF A PHYSICAL DEVICE CONTAINS AN AUTHENTICATION CERTIFICATE (DESKTOP)

InfoCert
TINEXTA GROUP

SUMMARY

1.1 OVERVIEW: WHY IS IT NEEDED?

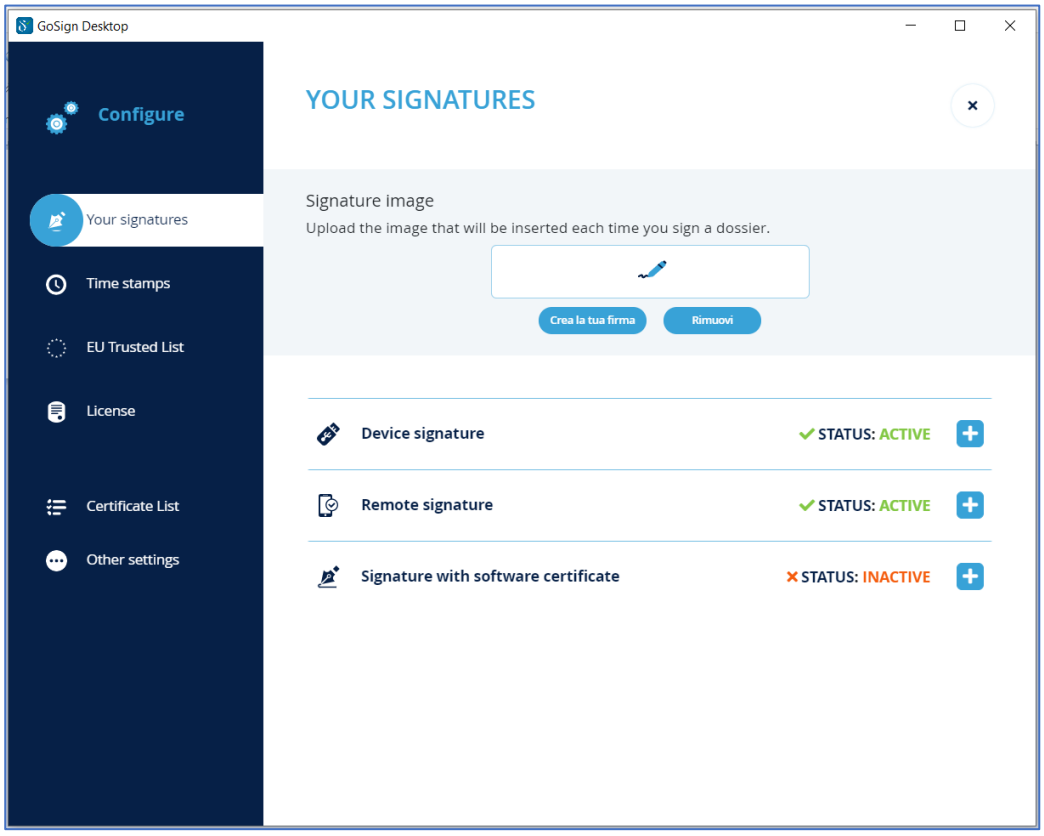
The **authentication certificate** allows the Controller to access the services provided on the network in a secure manner. It also allows you to sign or encrypt e-mail messages.

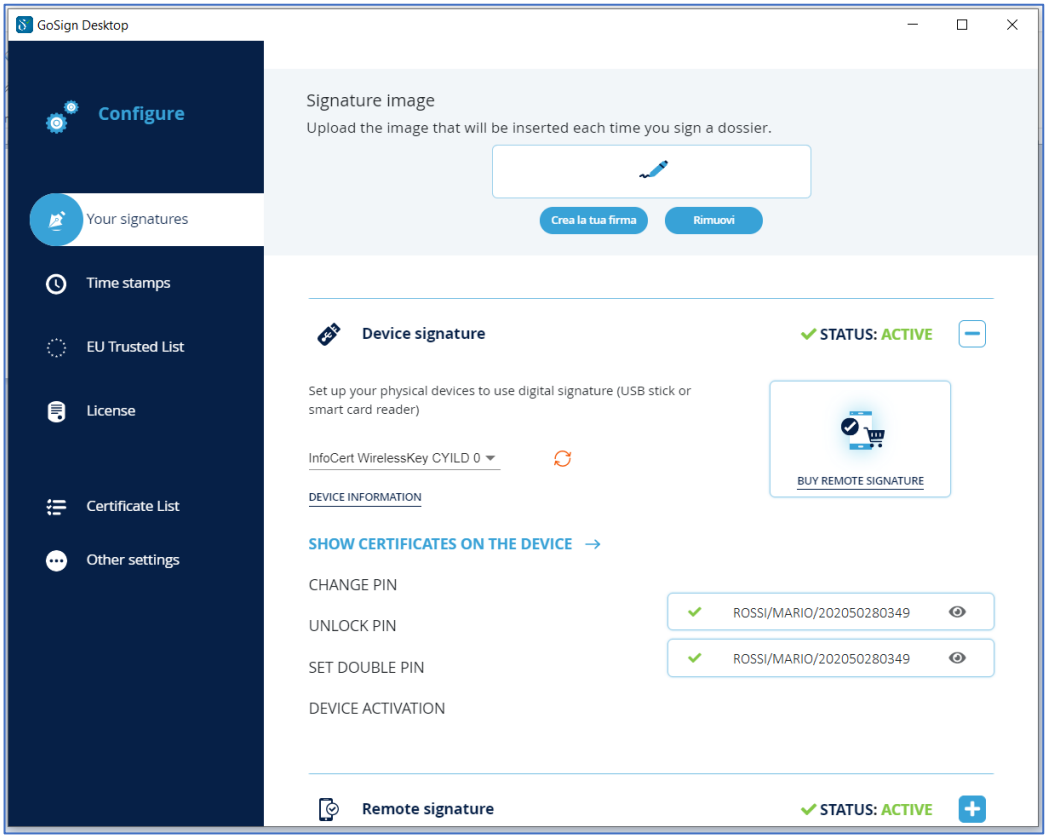
It is issued by a Qualified Trusted Service Provider following the provisions of the **Operating Manual**. It provides for the certain identification of the Holder by the certifier but does not have a predefined technical standard.

1.2 ACTIVITY START: HOME PAGE

Double-clicking on the icon starts the **GoSign Desktop** program. Once the home page is displayed, you need to move to the **Configure** side menu (marked by the gear icon)**.**

Next, select the dedicated page ***Your signatures*** in the **device signature** section.





By selecting the *Show certificates on the device* function. The list of certificates contained within the device will appear on the right side:

- the certificate marked with a green icon and indicated with my name and surname is the signature certificate;
- the certificate marked with a yellow icon and the sequence **surname / name / IUT** (or Unique Identification of the certificate) is my authentication certificate.

If the sequence **Tax Code / serial number of the device / hash** is present next to the yellow icon, it means that a CNS type authentication certificate is present on the device.