Registration Authority

Remote Signature Guide for Web

Category	**TSP-Digital Signature**	Document Code	**NAM-Remote Signature for Web**	**Namirial S.p.A.**
Prepared by	**Michelangelo Bonvini**	Confidentiality note	**Public Document**	Registration Authority
Verified by	**Gabriele Bocchini**	Version	**1.0**	**Gabriele Bocchini**
Approved by	**Gabriele Bocchini**	Date of issue	**01/05/2020**	_____

Namirial S.p.A.

Registered offices, management and administration headquarters 60019 Senigallia (AN) - via Caduti sul Lavoro, 4
TAX CODE/ANCONA REG. OF COMPANIES NO. 02046570426 - VAT NO. IT02046570426 - SHARE CAP. € 6,500,000.00 fully paid-up
Tel. 07163494 hotline - Fax 199.418016 - info@namirial.com - www.namirial.com

UNI EN ISO 9001:2015 - Certificate No. 223776 | **UNI EN ISO 27001:2013** - Certificate No. IT280490

– This page is intentionally left blank –

TABLE OF CONTENTS

Table of contents **3**

History of changes **4**

1 Introduction **5**

1.1 Purpose of the document and field of application 5

1.2 Definitions and Acronyms used in the document 5

2 Go to the Private Area **6**

3 How to Sign a File **6**

4 How to Verify a File **8**

5 Management **9**

Index of Tables **11**

Index of Figures **11**

HISTORY OF CHANGES

VERSION	**1.0**
Date	01/05/2020
Reason	Updating the document with new software screenshots
Changes	---

1 INTRODUCTION

1.1 PURPOSE OF THE DOCUMENT AND FIELD OF APPLICATION

This document is a "quick guide" to using and managing the Remote Digital Signature to be used in the Namirial private area.

A Remote Signature is a specific type of digital signature based on OTPs, i.e. temporary passwords that expire a few seconds after they are generated, thus eliminating the risks associated with using static passwords.
The signature certificate is not held on a Hardware device but is instead installed on a HSM (Hardware Security Module) managed by the Namirial Certification Authority.
The Remote Signature system guarantees extremely high levels of service security and availability and offers the option of using the service on Desktop or Mobile systems.

1.2 DEFINITIONS AND ACRONYMS USED IN THE DOCUMENT

TERM	MEANING
Digital Signature	is a specific type of qualified electronic signature and represents the set of data in electronic form, which is attached to or logically associated with other data in electronic form, used as an electronic identification method.
Remote Signature	The **Remote Digital Signature** process optimises digital signature functionality but is based on **OTPs**, i.e. temporary passwords that **expire a few seconds after they are generated,** thus eliminating the risks associated with using static passwords.
Namirial OTP	Namirial OTP is an application for mobile devices that enables the use of **One Time Passwords**.
HSM	(Hardware Security Module) managed by the Namirial Certification Authority.
Base64	is a positional numbering system that uses 64 symbols. It is mainly used to encode binary data in e-mails and to convert data into ASCII format. Base64 encoding results in a 33% overall increase in the size of the data to be decoded.
<…>	<…>

Table 1 - Definitions and Acronyms

2 GO TO THE PRIVATE AREA

Log on to your Reserved Area at https://portal.namirialtsp.com/ and click **Access**.
Alternatively, you can log on by following the link contained in the e-mail you received with your Private Area details.

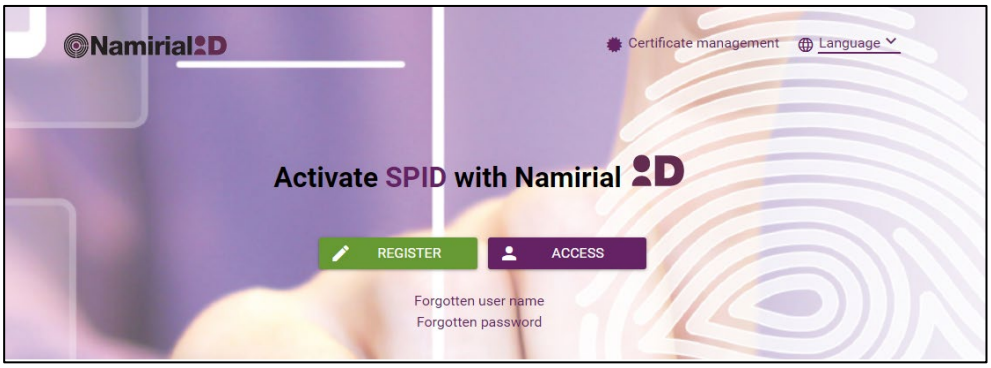


Figure 1 - Private Area Homepage

RECOVER PRIVATE AREA CREDENTIALS: *Users who have lost their username and/or password can recover the individual details by clicking "Forgotten Username" or "Forgotten Password" and following the instructions provided. If the problem persists, contact technical support at support.dts@namirial.com with the following information in the SUBJECT LINE:* ***RECOVER PRIVATE AREA CREDENTIALS*** *– Tax code.*

3 HOW TO SIGN A FILE

The new function implemented in the Private Area allows all users with a remote digital signature certificate to digitally sign any file *without installing any software or drivers, because the entire process takes place in the web portal.*
This function can be accessed from the menu on the left, by going to: *[User] > [Digital Signature] > [Signature];*

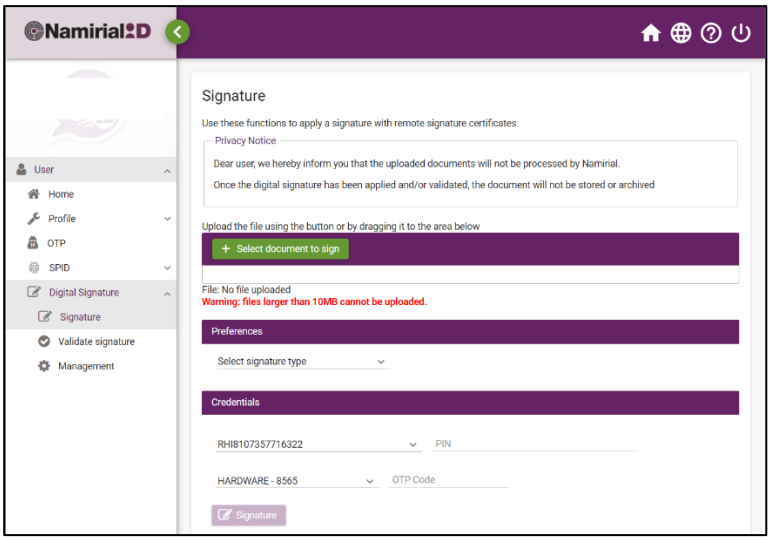
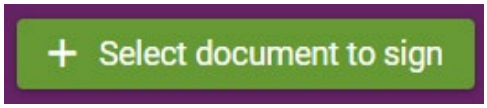
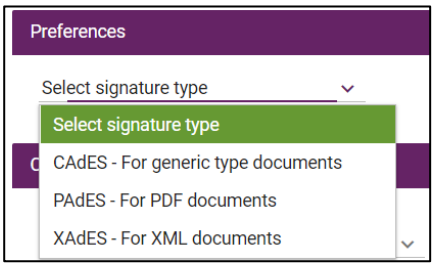


Figure 2 - How to sign



From the Firma [Sign] menu, click the green button marked ***Seleziona documento da firmare*** [Select document to sign] and search the folders on your PC to find the file you wish to sign.

Figure 3 - select file

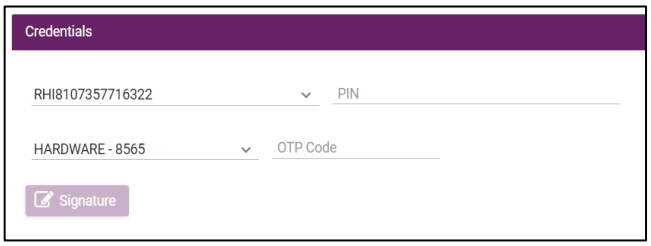


From ***Preferenze*** [Preferences], users can select from among the signature formats available for that file type.

- *CAdES*: sign the file using the .p7m format
- *PAdES*: sign the file while maintaining the .pdf format
- *XAdES*: sign the file while maintaining the .xml format

ATTENTION:
if the XAdES format is selected, users have the option to sign the whole xml file, or just one element of it, by specifying the ID.

Figure 4 - select signature type



From the section marked ***[Credentials]***

1. Select the remote signature device to use;
2. Select the OTP token type to use;
3. Enter the PIN Code and the OTP Code generated (SMS – HARDWARE – VIRTUAL).
4. Press the [Sign] button.
5. The signed document can be downloaded once the process is complete.

Figure 5 - signing process.

ATTENTION:

- The PIN code is provided in the Digital Security Envelope, received by e-mail.
- In the case of certificates *Issued by the Holder* only, the relevant PIN code is the one set during the certificate issue process.
- If the client has multiple remote digital signatures, the certificate to be used can be selected by going to [Select Signature Device].
- If the client has multiple OTP tokens, the OTP token to be used can be selected by going to [Select OTP Token].

OTP TOKEN CONFIGURATION

Before proceeding with the signing process, holders of Hardware OTP Tokens and Virtual OTP Tokens must ensure that these have been properly configured:

- For Virtual OTP Token holders:
  - See iOS config: Namirial-otp iOS
  - See Android config: Namirial-otp Android
- For Hardware OTP Token holders: [Configuring OTP Hardware Token].

4 HOW TO VERIFY A FILE

The new function implemented in the Private Area allows users to verify the validity of any file *without installing any software or drivers, because the entire process takes place in the web portal.*

This function can be accessed from the menu on the left, by going to: [User] > [Digital Signature] > [Validate Signature]

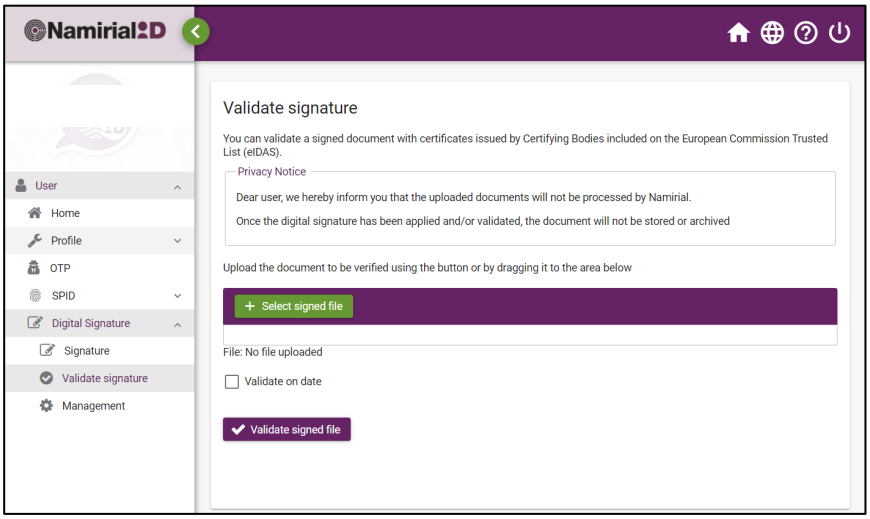


Figure 6 - how to verify a file

Figure 7- select verified file

From the Firma [Sign] menu, click the green button marked [**Select signed file**] and search the folders of your PC to find the file you wish to verify.

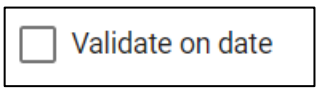


Figure 8 - validate on date

Attention: Select [Validate on date] to specify a date for the verification process to begin.

Having loaded the file to verify, click **Validate signed file** to view the result of the validation process.

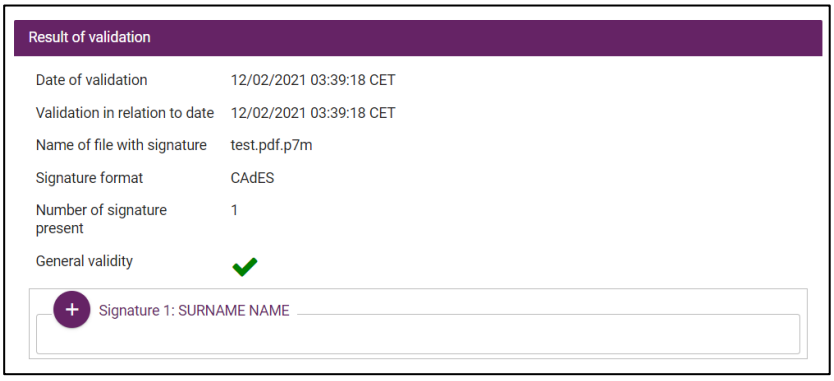


Figure 9 - result of validation process

5 MANAGEMENT

The Management section lets users verify all digital signature certificates issued by Namirial and held by the User, and carry out certain operations on the certificate that will be explained here below.

To access these functions, go to: *[User]* > *[Digital Signature]* > *[Management]*

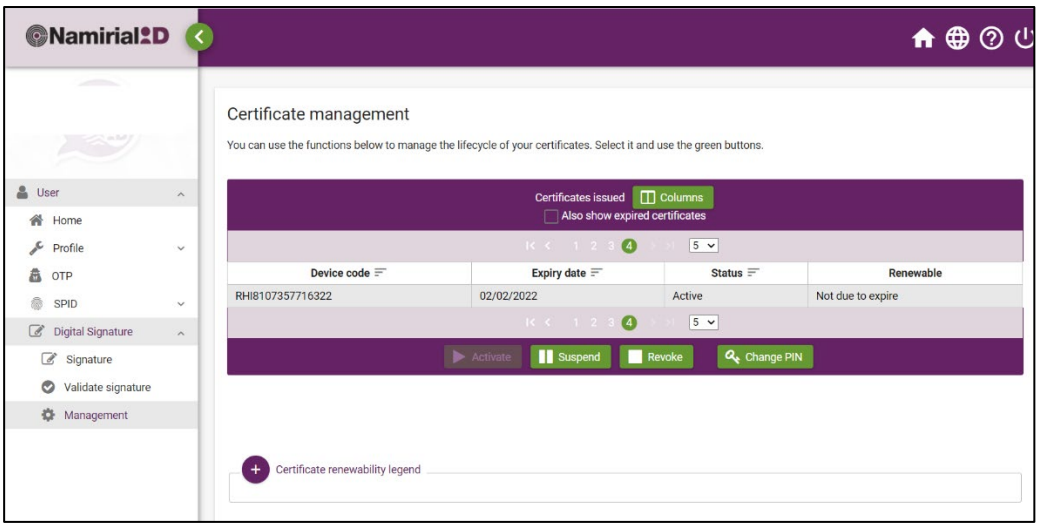
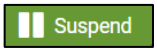


Figure 10 - manage signature

ATTENTION: *An additional OTP-based security level is required to access this section of the portal. Users with multiple OTP tokens issued by Namirial can select which token to use.*



Suspension of a Digital Certificate is requested in all cases where validity of that certificate must be interrupted.
Example:

- To comply with orders issued by an authority
- Due to factors that limit the capacity of the holder, or in cases of misuse or forgery
- If the certificate or the codes are lost

Suspension can be requested by the Certificate Holder, the Interested Third Party or an Authority.

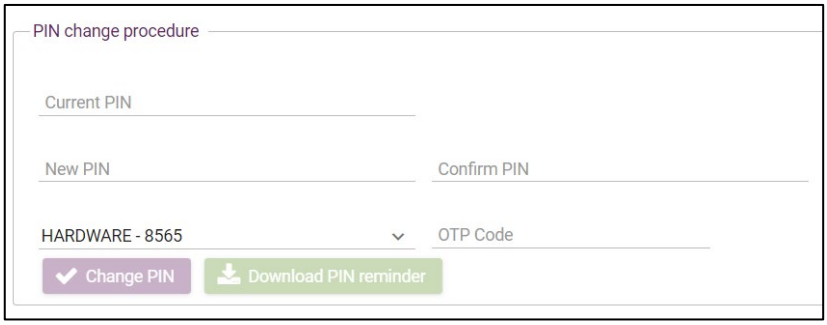
Figure 11 - suspend certificate

Revoking a Digital Certificate is an irreversible operation that invalidates the use of that certificate from the moment it is performed. The operation should only be performed if absolutely necessary.

Figure 12 - revoke certificate

The Activate function is only available if the certificate is Suspended.

Figure 13 - activate certificate



In the section marked ***[PIN change procedure]***

1. Enter the PIN provided by Namirial (if a digital security envelope was used)
2. Enter the new PIN;
3. Confirm PIN;
4. Select the OTP token type to use;
5. Enter the PIN Code and the OTP Code generated (SMS – HARDWARE – VIRTUAL).
6. Press the button marked **[Change PIN]**;
7. When the procedure is complete, the user can download a PIN reminder (Recommended Option, as Namirial does not keep a record of the PIN and a new signature certificate must be requested if the PIN is forgotten)

Figure 14 - change PIN

By clicking "" [Columns], the user can select which columns to view for the certificates issued in his/her name.

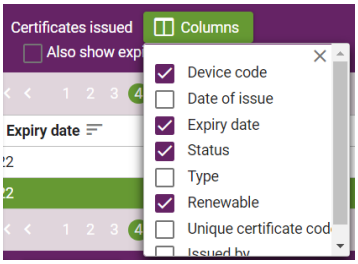


Figure 15 - manage columns

INDEX OF TABLES

Table 1 - Definitions and Acronyms 5

INDEX OF FIGURES

Figure 1 - Private Area Homepage 6

Figure 2 - How to sign 6

Figure 3 - select file 7

Figure 4 - select signature type 7

Figure 5 - signing process 7

Figure 6 - how to verify a file 8

Figure 7- select verified file 8

Figure 8 - validate on date 8

Figure 9 - result of validation process 9

Figure 10 - manage signature 9

Figure 11 - suspend certificate 9

Figure 12 - revoke certificate 10

Figure 13 - activate certificate 10

Figure 14 - change PIN 10

Figure 15 - manage columns 10