ActalisCodeSigner

ActalisCodeSigner is a command-line application that provides functionality for signing executable and script files by a code signing user.

Installation

ActalisCodeSigner is a portable application, you can install it by extracting the archive in any directory of your system.

This way you can interact with the application, from command line, by moving inside the directory where **ActalisCodeSigner** executable (**ActalisCodeSigner.exe** on Windows) is located and by launching the supported command.

PATH Integration

It is possible to add the installation folder to the PATH environment variable to use the tool from any location.

Warning: The executable relies on the working directory set by the calling shell to locate its dependencies. Therefore, it is necessary to define a script within the same folder, such as the following:

```
@echo off
Pushd %~dp0
actaliscodesigner.exe %*
popd
```

Then, the script should be called with the respective parameters instead of the original executable.

Requirements

ActalisCodeSigner is released for Windows and Linux.

Reaching of the following endpoint is required:

- https://app1.firma-remota.it/ArubaSignerService/webresources/signerservice
- https://app2.firma-remota.it/ArubaSignerService/webresources/signerservice
- http://timestamp.actalis.com

and other defined by parameters from the user.

Actalis S.p.A.
Via San Clemente 53, Ponte San Pietro 24036 (BG)
VAT Reg. No. 03358520967 | **Tax ID No.** 03358520967
REA [Administrative and Economic Index] 436479 | **Share Capital** € 6,300,000.00 fully paid up |
Certified email: amministrazione@pec.actalis.it | **Website** actalis.com

Signature credentials

Remote signature's credentials will be provided to apply signature.

Password updates is mandatory, using **Change Password** feature, before using it.

Signing with expired credential will result in the following error:

```
KeyStore creation error: Password Expired
```

Supported format

ActalisCodeSigner can sign the following formats:

- eseguibili: **exe (*), msi, jar**
- script: **ps1, psd1, psm1, ps1xml, vbs, vbe, js, jse, wsf**

Support outside of these contexts is not guaranteed (see the "Known Limitations" section for more details).

Some formats are handled by the tool even though they are not explicitly listed among the supported ones:

- The **DLL** format is generally treated like an **EXE** and managed by the tool accordingly.
- The **WAR** format is treated as a **JAR**.

Usage

You can select different signature configuration by giving different input parameters.
In the examples we use short parameters for brevity.

Signature

Base signature mode is

```
ActalisCodeSigner.exe -fu username -fp password -in /path/to/fileToSign.exe
```

this way a signature is applied to *fileToSign.exe*

If you want to preserve the original file, you can specify output file path

```
ActalisCodeSigner.exe -fu username -fp password -in /path/to/fileToSign.exe -out
/path/to/signedFile.exe
```

this way the signature is applied to signedFile.exe and the original file is left unaltered.

Signature with time stamp

With **ActalisCodeSigner** you can also apply a time stamp together with the signature

```
ActalisCodeSigner.exe -fu username -fp password -in /path/to/fileToSign.exe -ts
```

-ts parameter indicate to apply time stamp with the signature. To use a different time stamp services from default (http://timestamp.actalis.com/) you can specify it after the parameter.

For example, if you want to use https://url.tsa.com/ services (NB. this url is not related to a TSA services)

```
ActalisCodeSigner.exe -fu username -fp password -in /path/to/fileToSign.exe -ts
https://url.tsa.com
```

If TSA services require authentication, you can provide credentials by **-tu** and **-tp** parameters

```
ActalisCodeSigner.exe -fu username -fp password -in /path/to/fileToSign.exe -ts
https://url.tsa.com -tu username_tsa -tp password_tsa
```

Network configuration

ActalisCodeSigner supports connection to signing and time stamp services via proxy. Proxy configuration can be specified with **-pu** and **-pp** parameters

For example, with a proxy url http://127.0.0.1

```
ActalisCodeSigner.exe -fu username -fp password -in /path/to/fileToSign.exe
http://127.0.0.1 -pu username_proxy -pp password_proxy
```

If proxy is set at system level, you can provide **-pa** parameter to specify to look up the proxy automatically.

```
ActalisCodeSigner.exe -fu username -fp password -in /path/to/fileToSign.exe -pa
```


Change password

The following command allows you to change the signature user's password

```
ActalisCodeSigner.exe -cp -fu username
```

After executing the command, you will be prompted to enter your current password and the new password.

NB: The codesign account is created with an expired password to force the user to change it before starting the signing activity.

Other parameters

Below is the table with the exhaustive list of all supported parameters and a brief description.

NB. unless otherwise specified the parameters are optional

Short parameter	Full parameter	Description
-pm	**--program-name**	Additional signature field
-ts	**--timestamp**	Apply time stamp, if present, you can specify time stamp services url optionally
-fd	**--fr-domain**	Code signing domain
-fo	**--fr-otp**	Code signing OTP
-fp	**--fr-password**	Code signing password, **mandatory** parameter
-fr1	**--fr-url1**	Code signing sevices primary url
-fr2	**--fr-url2**	Code signing sevices secondary url
-fu	**--fr-user**	Code signing user name , **mandatory** parameter
-in	**--input**	File to sign path, **mandatory** parameter
-h	**--help**	Print guide
-pa	**--proxy-auto**	Proxy server configuration is searched automatically, if present
-pp	**--proxy-password**	Proxy server password
-pu	**--proxy-user**	Proxy server user name
-da	**--digest-algorithm**	Signature's digest algorithm, SHA-256 is used if not present Supported values are MD5, SHA1, SHA-256, SHA-384, SHA-512
-out	**--output**	Signed file path, signature is applied in place on input file if absent
-tp	**--tsa-password**	Time stamp services password, only used if **--timestamp** is also present
-tu	**--tsa-user**	Time stamp services user name, only used if **--timestamp** is also present

Log e debug

Actalis S.p.A.
Via San Clemente 53, Ponte San Pietro 24036 (BG)
VAT Reg. No. 03358520967 | **Tax ID No.** 03358520967
REA [Administrative and Economic Index] 436479 | **Share Capital** € 6,300,000.00 fully paid up |
Certified email: amministrazione@pec.actalis.it | **Website** actalis.com

The tool creates a log file at the **INFO** level inside the following folder:

<userhome>/.Acsi/log

It is possible to enable detailed logging by adding the following property file in the **<userhome>/.Acsi** folder:

acsi.properties

And updating the property as follows:

```
core.logLevel=DEBUG
```

Known Limitations

Manifest Signing

Currently, the tool does not support signing manifest files generated by Visual Studio (and other IDEs).
If the generated application requires signing in this manner, it must be handled using a **p12** or a similar keystore, integrating it directly into the IDE at the end of the build process.

Obsolete Digest Algorithms

The **SHA1** (and **MD5**) algorithm for signature digest has been deprecated for security reasons in the following versions of Java.

- 17.0.5
- 11.0.17
- 8u351
- 7u361

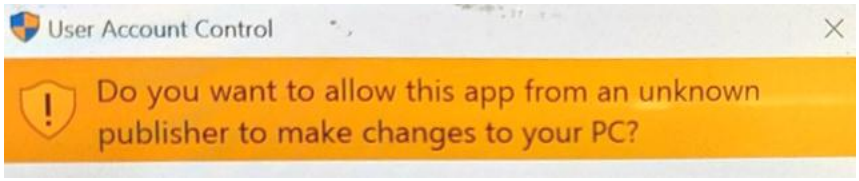
ActalisCodeSigner uses an embedded Java 17 version higher than the one specified. As a result, when signing a JAR file with the parameter -da SHA1, the following error occurs: "Unable to sign document". However, **SHA1** is still allowed for signing **EXE** and **MSI** files.

Signing MSI/EXE on Machines with Limited Network Access

Actalis S.p.A.
Via San Clemente 53, Ponte San Pietro 24036 (BG)
VAT Reg. No. 03358520967 | **Tax ID No.** 03358520967
REA [Administrative and Economic Index] 436479 | **Share Capital** € 6,300,000.00 fully paid up |
Certified email: amministrazione@pec.actalis.it | **Website** actalis.com

Executing signatures from PCs where online access is restricted by a proxy/firewall to whitelisted URLs only may negatively impact the subsequent validation of signed artifacts.

When the signature is present but validation fails, a **UAC warning dialog** appears.



which displays "Unknown" as the author.

It is recommended to verify the full accessibility of the machine performing the codesign or to test the signing process from a different machine.

Exit Code

The following exit codes have been introduced:

code 0 → Success

code 1 → Generic Error

code 2 → Credential Error

code 3 → Network Error

code 4 → Remote Signer Error

code 5 → Signature Error

Actalis S.p.A.
Via San Clemente 53, Ponte San Pietro 24036 (BG)
VAT Reg. No. 03358520967 | **Tax ID No.** 03358520967
REA [Administrative and Economic Index] 436479 | **Share Capital** € 6,300,000.00 fully paid up |
Certified email: amministrazione@pec.actalis.it | **Website** actalis.com