

ActalisCodeSigner

ActalisCodeSigner è un client a riga di comando che offre la possibilità di firmare file eseguibili e script mediante un'utenza di code sign.

Installazione

ActalisCodeSigner è un software portable, l'installazione richiede che venga estratto il contenuto dell'archivio dell'applicazione in una qualsiasi cartella del sistema.

In questo modo è possibile utilizzare il software, tramite riga di comando, spostandosi nella cartella in cui è presente l'eseguibile **ActalisCodeSigner** (**ActalisCodeSigner.exe** per Windows) e lanciando il comando desiderato.

In alternativa è possibile aggiungere la cartella alla variabile di ambiente **PATH** per poter usare il tool da qualsiasi posizione.

Requisiti

Il tool viene al momento prodotto per i contesti Windows e Linux.
E' richiesto il corretto raggiungimento dei seguenti endpoint:

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

oltre ad eventuali definiti in modo specifico tramite parametri.

Credenziali di firma

Per l'applicazione della firma remota vengono fornite apposite credenziali.

Prima di utilizzarle è necessario aggiornare la password mediante la funzionalità [Cambio Password](#)

Tentando di firmare con la password scaduta si riceverà l'errore:

Errore nella creazione del KeyStore: Password Expired

Formati supportati

Il tool riconosce e firma i seguenti formati

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

Non è garantito il supporto al di fuori di questi contesti.

Il formato **dll** è generalmente assimilato all'exe e gestito dal tool come tale.

Utilizzo

In base ai parametri forniti in input è possibile configurare la modalità di apposizione della firma.
Negli esempi riportati in questa pagina verranno usati sempre i parametri sintetici per brevità.



Firma

La modalità di base è la seguente:

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

In questo modo verrà applicata una firma al file *fileToSign.exe*

Nel caso si volesse mantenere inalterato il file originale è possibile fornire in input il path del file firmato

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

In questo modo si ottiene in output un nuovo file chiamato *signedFile.exe* contenente la firma.



Firma con marcatura temporale

ActalisCodeSigner fornisce la possibilità di aggiungere anche una marcatura temporale alla firma

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

Il parametro **-ts** indica che oltre alla firma deve essere applicata la marcatura temporale, se si volesse utilizzare un servizio di marcatura differente da quello di default (<http://timestamp.actalis.com>) è possibile inserirlo come valore del parametro.

Ad esempio, se si volesse usare il servizio <https://url.tsa.com> (NB. l'url è solo di esempio e non è collegato ad un servizio di TSA)

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

Se il servizio di marcatura temporale richiede delle credenziali per l'autenticazione, è possibile fornirle tramite i parametri **-tu** e **-tp**

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



Configurazione di rete

ActalisCodeSigner supporta la connessione ai servizi di firma e marcatura tramite proxy.

La configurazione del proxy può essere fornita tramite i parametri **-pr**, **-pu**, **-pp** e **-po**

Ad esempio, se il proxy fosse raggiungibile all'url <http://127.0.0.1>

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

In caso di proxy configurato a livello di sistema, è possibile sfruttare il parametro **-pa** per indicare ad **ActalisCodeSigner** di eseguire una ricerca automatica sui proxy presenti

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

Cambio password

Il seguente comando permette la modifica della password associata all'utenza di firma

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

Successivamente all'esecuzione del comando verrà richiesto l'inserimento della password attuale e della nuova password

Altri parametri

Di seguito è riportata la tabella con l'elenco esaustivo di tutti i parametri supportati e una breve descrizione.

NB. se non diversamente specificato i parametri sono opzionali

| Parametro sintetico | Parametro completo | Descrizione |
|---------------------|----------------------|---|
| -fu | --fr-user | nome utente di code signing, è un parametro obbligatorio |
| -fp | --fr-password | password di code signing, è un parametro obbligatorio |
| -fd | --fr-domain | dominio dell'utenza di code signing di code signing |
| -fo | --fr-otp | codice OTP dell'utenza di code signing |
| -fr1 | --fr-url1 | url primario del servizio di code signing |
| -fr2 | --fr-url2 | url secondario del servizio di code signing |
| -in | --input | path del file da firmare, è un parametro obbligatorio |

| Parametro sintetico | Parametro completo | Descrizione |
|---------------------|---------------------------|---|
| -out | --output | path del file firmato, se non presente la firma viene apposta direttamente sul file di input |
| -ts | --timestamp | se il parametro è presente, applica la marcatura temporale, opzionalmente è possibile fornire anche l'url del servizio di marcatura temporale |
| -tu | --tsa-user | user dell'endpoint del servizio che esegue la marcatura temporale, usato solo se è presente anche --timestamp |
| -tp | --tsa-password | password dell'endpoint del servizio che esegue la marcatura temporale, usato solo se è presente anche --timestamp |
| -pm | --program-name | campo aggiuntivo di informazioni inseriti nella firma |
| -pr | --program-url | campo aggiuntivo di informazioni inseriti nella firma |
| -da | --digest-algorithm | algoritmo di digest utilizzato per la firma, se non valorizzato verrà utilizzato SHA-256 I valori supportati sono MD5, SHA1, SHA-256, SHA-384, SHA-512 |
| -pr | --proxy-url | url del proxy |
| -pu | --proxy-user | username del proxy |
| -pp | --proxy-password | password del proxy |
| -pa | --proxy-auto | se il parametro è presente, il proxy viene individuato automaticamente |
| -h | --help | stampa la guida |

Log e debug

Il tool crea un file di log a livello INFO all'interno della cartella

<userhome>/.Acsi/log

E' possibile impostare un log di dettaglio inserendo nella cartella <userhome>/.Acsi il seguente file di property:

[acsi.properties](#)

e aggiornando la property come segue

```
core.logLevel=DEBUG
```

Limiti noti

Firma di manifest

Al momento il tool non supporta la firma di file manifest generati da Visual Studio (e altri IDE).

Se l'applicativo generato richiede la firma in tal senso occorre provvedere tramite p12 o altro store analogo integrandolo direttamente nell'IDE al termine della fase di build.

Algoritmi digest obsoleti

L'algoritmo SHA1 (e il MD5) come algoritmo di digest nella firma è stato deprecato per motivi di sicurezza dalle seguenti versioni di Java

- 17.0.5
- 11.0.17
- 8u351
- 7u361

ActalisCodeSigner utilizza una Java embedded 17 superiore a quella indicata e quindi applicando la firma ad un file jar con il parametro "-da SHA1" si ottiene un errore "Unable to sign document".

Lo SHA1 è invece ammesso nel caso di firme di exe e msi.