



# Firma degli eseguibili Windows

David Lastrucci  
Open Source Italia S.r.l.





# David Lastrucci

- Sviluppo in Delphi (e non solo) fino dalla sua prima versione
- In OSItalia (Open Source Italia S.r.l.) faccio parte del Team di Ricerca & Sviluppo e sono responsabile dei componenti ed i wizard utilizzati per lo sviluppo del Software Gestionale OS1

[david.lastrucci@ositalia.com](mailto:david.lastrucci@ositalia.com)


[david.lastrucci@gmail.com](mailto:david.lastrucci@gmail.com)

Skype: david.lastrucci






# Firma degli eseguibili Windows

- Perché firmare gli eseguibili
  - Certificati di firma
  - Windows 10 SDK
  - Tipologie di firma
  - Timestamp
  - Firma
  - Controllo della firma
- 




## Perché firmare gli eseguibili

- La firma del software (code sign) garantisce:
    - L'autore del software
    - L'autenticità del software
  - Dimostra che il software è integro ed affidabile (integro di sicuro, affidabile non è certo)
- 

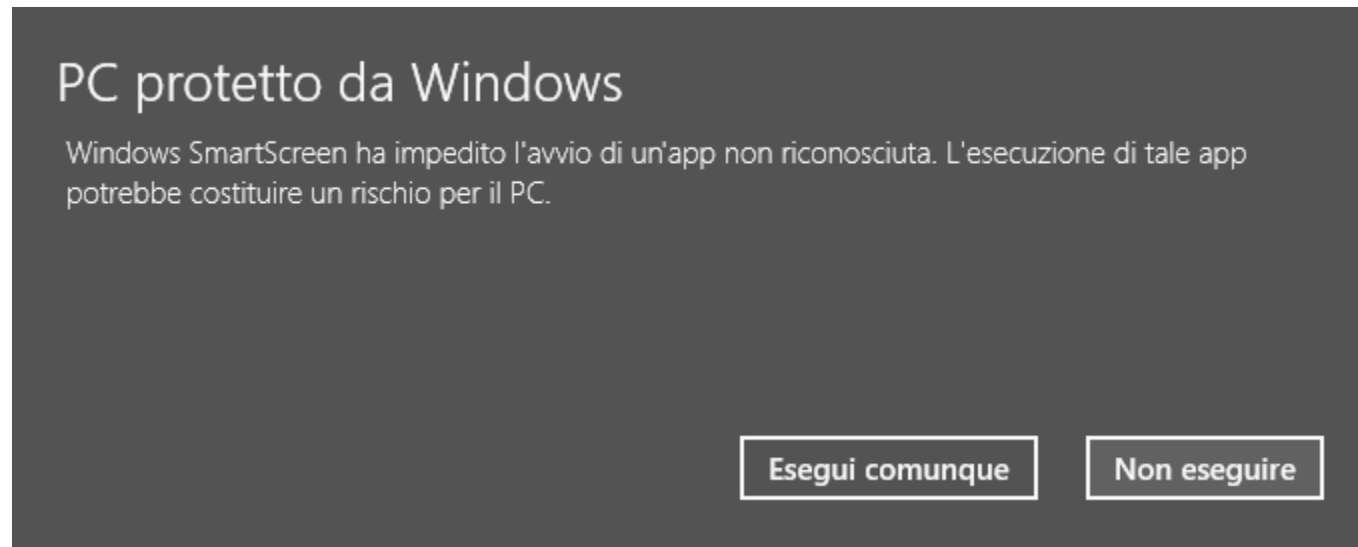


## Certificati di firma

- Esistono due tipologie di certificati per la firma del codice: Regular ed EV (Extended Validated)
  - I certificati EV sono obbligatori per la firma dei Driver
  - Per gli altri software sono sufficienti i certificati regolari
  - I certificati EV richiedono una certificazione aziendale (non vengono rilasciati a singoli sviluppatori)
- 

# Certificati di firma

- Con i certificati EV viene bypassato automaticamente il filtro SmartScreen di Windows (la reputazione è immediata alla firma del software)





## Certificati di firma

- I certificati di firma devono essere acquistati da aziende CA (Certification Authority)
- Possono, ad esempio, essere acquistati da:

<https://www.digicert.com/code-signing>

<https://comodossllstore.com/codesigning.aspx>





# Windows 10 SDK

- Per la firma degli eseguibili è necessario installare **Windows 10 SDK**

<https://developer.microsoft.com/it-it/windows/downloads/windows-10-sdk>

- Del Kit Microsoft andremo ad utilizzare signtool.exe

<https://docs.microsoft.com/it-it/dotnet/framework/tools/signtool-exe>







# Windows 10 SDK

- Useremo anche:

- makecert.exe per creare un certificato self signed

<https://docs.microsoft.com/en-us/windows/win32/seccrypto/makecert>

- pvk2pfx.exe per convertire il certificato in formato pfx (Personal Information Exchange) che è quello che ci serve

<https://docs.microsoft.com/en-us/windows-hardware/drivers/devtest/pvk2pfx>



# Tipologie di firma


- La firma degli eseguibili Windows può essere SHA1 o SHA256
- Attenzione alle versioni del Sistema Operativo:

Sistema Operativo	SHA1	SHA256
Windows XP / Windows Server 2003	Sì	No
Windows Vista / Windows Server 2008	Sì	No
Windows 7 / Windows Server 2008 R2	No*	Sì
Windows 8.1 / Windows Server 2012 R2	No*	Sì
Windows 10 / Windows Server 2016	No*	Sì

\* SHA1 è supportato se la data della firma è precedente al 01/01/2016



# Timestamp

- Il timestamp estende l'attendibilità del software oltre il periodo di validità del certificato
  - In pratica se il timestamp attesta che la firma è stata apposta precedentemente alla revoca del certificato, il software rimane attendibile anche se il certificato risulta scaduto o revocato
  - Il timestamp può essere aggiunto anche in un secondo tempo, dopo la firma dell'eseguibile
- 

# Firma

- Per apporre la firma ad un software, si usa:

```
signtool.exe  
  sign  
    /fd [sha1|sha255]  
    /f [Certificato.pfx]  
    /p [Password]  
    /t [Url]  
    [Programma]
```


# Firma

- Per apporre una nuova firma ad un software già firmato, si usa:

```
signtool.exe  
    sign  
    /fd [sha1|sha256]  
    /f [Certificato.pfx]  
    /p [Password]  
    /tr [Url]  
    /as  
    [Programma]
```



## Controllo della firma

- Di un software possiamo sapere:
    - Se è firmato digitalmente
    - Chi è l'intestatario del certificato di firma
- 



# Materiale

- Su GitHub potete trovare tutto il materiale:
  - Le slide
  - I batch
  - I due esempi Delphi

<https://github.com/davidlastrucci/delphilive2020>

