Il tool XCZ

Questa procedura mostra come creare una CA tramite il tool XCA e come firmare altri certificati.

- 1) Aprire il programma XCA.
- 2) Creare una nuova chiave:

| 📴 Creare una CA (certification autority).doc - Microsoft Word | _ B × |
|---|---------------------------|
| i Elle Modifica Yisualizza Inserisci Figmato Strumenti Tabella Figestra 2 Adobe PDF Commenti Acrobat | Digitare una domanda. 🔹 🗙 |
| 🗓 📴 🛃 👌 🔄 🕄 🕄 🕺 🕹 💫 🖏 🥙 + 🔍 + 🧶 😼 📰 🖓 🖏 📲 🛷 🕄 🖉 💷 Letture 👷 🔁 🏗 🖏 💂 | |
| ▲ Normale • Times New Roman • 12 • G C S ■ 著 書 篇 + 1 注 注 译 译 □ • 12 • Δ •] | |
| 20111 >- X Certificate and Key management | |
| File Import Help | |
| Private Keys Certificate signing requests Certificates Templates Revocation lists | |
| Name A Type Size Use Password New Key | |
| Keyket RSA L024 bit 2 Common | |
| Import | |
| Import PEX (PECS#12) | |
| | |
| | |
| - Dece | |
| Change password | |
| | |
| 2 Decense on forward the second provide the second | |
| | * * * |
| Disegno + | |
| Pg 1 Sez 1 1/1 A 2,9 cm Ri 2 Col 3 REG REV EST SSC Italano (Ital 🕰 | |
| 🦹 Start 🏽 🍘 🕘 👋 🔹 Java - ProvaReti/src/pr 🛛 🗫 X Certificate and Ke 🐒 KeyTool GUI 1.7 - [D:\ 🗋 D:\Documents and Sett 🗐 Facebook Govanni G 🗐 Creare una CA (certific | 🖌 🔍 🛃 🙆 🦹 🎑 🎘 🕲 15.21 |

cosi facendo il programma creerà automaticamente una coppi di chiavi (pubblica e privata).

3) Scegliere come meglio si crede i seguenti parametri:

| 🕎 Creare una CA (certification autority).doc - Microsoft | ord | |
|--|--|--|
| Eile Modifica Visualizza Inserisci Formato Strument | Iabella Finestra ? Adobe PDF Commenti Acrobat | Digitare una domanda. 👻 🗙 |
| i 🗋 📂 🛃 💪 🚑 i 🍜 🕰 i 🌮 🕰 i 👗 🖦 🛍 🤇 | 🔊 • (? •) 🧕 🧊 🛅 📷 🎟 🛷 🐺 ¶ 100% 🔹 🎯 📖 Lettura 📕 📆 | 西北 🗟 🖕 |
| A Normale • Times New Roman • 12 • | • cs ■書書■篇+ 註註譯譯 圖• [●] •▲•, | |
| L 2 · · · · 1 · 0- | Certificate and Key management | |
| T. Fi | Import Help | |
| N | rivate Keys Certificate signing requests Certificates Templates Revocation lists | |
| | Name 🛆 Type Size Use Password | |
| | KeyProva RSA 2048 bit 2 Common | New Key |
| 4 | KeyReti - New key | ?X port |
| | New key | port |
| <u>φ</u> | | K (PKCS#12) |
| u | Please give a name to the new key and select the desired keysize | Debala IIII |
| ÷ | Name New Yey | |
| N | Kaution 1024 bit | |
| დ | Keysice 1024 bit | password |
| | | |
| ۳. | | |
| - - | Court 1 | cutto I |
| | Cancei | |
| H. C. | | |
| 1. 12 | | |
| | | |
| | | |
| | abase:u:/Documents and Settings/killer/Desktop/databasekey.xdb | |
| | | |
| ÷. | | * |
| - - - | | • |
| | | |
| i Disegno 🔹 🔓 Eorme 🔹 🔪 🗖 🔿 🔛 🔌 🛟 🧕 | & 🌭 • 🚄 • 📥 • ≡ ☴ ☵ 💷 🗊 💂 | |
| Pg 1 Sez 1 1/1 A 15,5 cm Ri 7 Col 4 | REG REV EST SSC Italiano (Ital | |
| 🏄 Start 🏾 🏉 🚱 🧶 🔹 🍃 Java - ProvaReti/src/pr | - X Certificate and Ke 👫 KeyTool GUI 1.7 - [D:\ 🗁 D:\Documents and Sett 📢 | 🛛 Facebook Giovanni Ci 🛛 🖳 Creare una CA (certific 🗍 < 🛒 🕑 🔏 💽 👰 🚳 15.22 |

E premere OK

4) Dopo di che creiamo una richiesta di firma di un certificato:



5) settare nome della richiesta:

| 🖷 Creare una CA (certification autority).doc - Microsoft Word | | _ 8 × |
|---|--|---------------------------|
| Eile Modifica Visualizza Inserisci Formato Strumenti Iab | ella Finestra <u>?</u> Adobe PDF <u>C</u> ommenti Acrobat | Digitare una domanda. 🔹 🗙 |
| : D 💕 🖬 💪 🔒 i 🖨 🕰 i 🌮 📖 i 🛦 🗈 🛍 🕩 🤊 | → X Certificate and Key management | |
| A4 Normale Times New Roman 12 G C | | |
| ▶ 2 · · · 1 · 2 · · X Cert | Create Certificate signing request | • |
| Pile Impo | Source Subject Extensions Key Usage Netscape | |
| Private | | |
| - | | |
| Name | Signing request | |
| | unstructure ProvaGuida | |
| | demengePassword | |
| ii 🦯 | | |
| | | |
| Ċ. | -Signing | |
| | Create a self signed certificate with the serial | |
| | C Lice this Certificate for for signing | |
| ۰ ۳ | | |
| - | | |
| - | Construction in the second sec | |
| · · · | Signature algorithm | |
| - N | | |
| - | Template V | |
| ė. | Template for the new certificate [default] CA | |
| | | |
| | | |
| | | |
| - - | Cancel OK | |
| ¥. | | ▼ |
| | | • |
| ≡ Ģ ⊟ ½ ♀ ◀ | | × |
| Disegno + 🔓 Eorme + 🔪 🔪 🗔 🔿 🔛 🖂 | <u>></u> - <u>⊿</u> - ≡ ☴ ☴ □ □ | |
| Pg 2 Sez 1 2/2 A 3,4 cm Ri 3 Col 1 R | EG REV EST SSC Italiano (Ital 🛄 | |
| 🛃 Start 💋 🧐 🧐 🔹 👻 🍃 Java - ProvaReti/src/pr 🔛 🛪 Co | ertificate and Ke 👫 KeyTool GUI 1.7 - [D:\ 🗀 D:\Documents and Sett 🧐 Facebook Giovanni Ci 👜 Creare una CA (certific | . 🔍 🛒 🗿 🦹 🙆 👰 🗞 15.25 |

Dalla stessa finestra andare nel TAB Subject

6) Riempire i campi indicati:

| 🖫 Creare una CA (certification autority).doc - Microsoft Word | |
|---|-----------------------------|
| i Ejle Modifica Vjsualizza Inserisci Figmato Strumenti Iabela Figestra 2 Adobe PDF Commenti Acrobat | Digitare una domanda. 🛛 👻 🗙 |
| 🗋 📴 🛃 👌 🗇 🗳 🖏 🐇 🐂 🖏 🏈 🍼 🖂 X Certificate and Key management 🛛 😰 🗶 | |
| A Normale - Times New Roman - 12 - G C | |
| Create Certificate signing request | |
| File Tor Source | ۲ ۲ ۲ ۲ ۲ |
| | |
| | / =V =V @ Q @ @ 0 +E 74 |
| 🐨 start 🕐 🖉 🥣 🥣 start in start and start in the start and start an | 🐂 式 🗁 🗁 🗥 🐼 🏹 🖏 15.26 |

7) Dopo di che bisogna indicare l'estensione, cioe bisogna dire che il certificato che stiamo creando riguarda una certification autority, cioè è un certificato per firmare altri certificati cioè per garantire altri certificati:

| 🖳 Creare una CA (certification autority).doc - Microsoft Word | <u>_ 8 ×</u> |
|---|---|
| i Ejle Modifica Ysualizza Inserisci Formato Izrumenti Iabella Finjestra 2 Adobe PDF Commenti Acrobat | Digitare una domanda. 🛛 🗸 🗙 |
| 🗓 📴 🖟 👌 🗐 🥝 🕵 🌾 🕵 🗸 🏸 🕞 🖍 🖉 🖉 🖓 🔊 | |
| A Normale - Times New Roman - 12 - G C | |
| Create Ceptitieste signing request | - |
| Prove Subject Extensions Key Usage Netscape Prove Basic contraining Wey Usage Netscape Wey Usage Prove Certification Certification Authority Reticate Path whill OTITA Certification Authority Reticate Reticate Vote Vote Subject Alexandrey Identifier Not before Subject Alexandrey Identifier Not before Subject alexandrey name Edit Apply Not after Subject alexandrey name Edit Gause CCSP Edit Cincel | - - - - - - - - - - - - - - - - - - - |
| | |
| Pa 3 Sez 1 33 A RI Col REG REV EST SSC Italiano (Ital D2) | |
| 🐉 Start 🏽 🍘 🔞 👋 🥃 Java - ProvaRetijsrcjpr 📴 X Certificate and Ke 🐉 Key Tool GUI 1.7 - [D:\ 🗁 D:\Documents and Sett 😻 Facebook Govanni G 🗐 Creare una CA (certific 🔍 | 🛒 🗾 🧟 🦹 🙆 👰 🗞 15.33 |

8) Dopo di che ci autofirmiamo il certificato appena creato:

| 🕎 Creare una CA (certification autority).doc - Microsoft Word | |
|--|---|
| Ele Modifica Visualizza Inserisci Formato Strumenti Iabella Finestra ? Adobe PDF Commenti Acrobat | Digitare una domanda. 👻 🗙 |
| 🗄 🗋 🤪 🛃 💪 🗇 🛃 🐧 🖉 🔝 🐇 🖕 🏝 🔇 🏈 🔍 🔍 🔍 🕲 🚱 🖓 🙂 🕅 | |
| 1 <u>4</u> Normale 🗸 Times New Roman 🔹 12 💌 G C S 百 百 百 百 百 百 百 百 百 百 百 百 百 百 百 百 百 百 | |
| L 2 2 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 | |
| Private Keys Certificate signing requests Certificates Templates Revocation lists | |
| Name Subject A New Request | |
| CasaF New Request Export | |
| Import | |
| Rischi Show Details a Show Details | |
| Export Delete | |
| Delete | |
| | |
| | |
| | |
| | |
| Jerninete | |
| 8. - | |
| | |
| | |
| - Database:D:/Documents and Settings/Killer/Desktop/databasekey.xdb | |
| | |
| Temper 2 (Prove N N □ ○ 3 4 (2)) (2) 2 · 2 · A · E 田田田 2 / 2 · 2 · A · E 田田田 2 / 2 · 2 · A · E 田田田 2 / 2 · 2 · A · E · E · E · E · E · E · E · E · E | ▼ |
| | 0 |
| | |
| \exists Disegno + $\basel{eq:Disegno + baseline}$ Eorme + $\baseline \ \land \ \land \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $ | |
| Pg 3 Sez 1 3/3 A 16,4 cm Ri 9 Col 1 REG REV EST SSC Italiano (Ital 🕰 | |
| 🐒 Start 🖉 🎯 🥹 🔷 🍃 Java - ProvaReti/src/pr 🔛 🛣 X Certificate and Ke 🞳 Key Tool GUI 1.7 - [D:\ 🛅 D:\Documents and Sett 🕲 Facebook Giovanni Ci | 🖳 Creare una CA (certific 🛛 « 🕵 🛃 🙆 🧏 🎯 🎊 🚳 15.34 |

| 📴 Creare una EA (certification autority).doc - Microsoft Word | _ <u>- 8 ×</u> |
|--|---------------------------|
| Elle Modifica Visualizza Inserisci Formato Strumenti Iabella Figestra 2 Adobe PDF Commenti Acrobat | Digitare una domanda. 🔹 🗙 |
| 🗋 🖆 🖟 🞝 🗇 🎒 🎝 🖓 🏭 🐇 🛍 🖏 🌮 X Certificate and Key management 🛛 🛐 🛛 | |
| 4 Normale Times New Roman ≥ 12 ≥ G C | |
| L Create XSUS Certificate | • |
| File Impl Source Extensions Key Usage Netscape | |
| Private | |
| | |
| Signing request | |
| 🖞 🔽 Sign this Certificate signing request 🛛 GuidaProva 💌 📃 | |
| Copy extensions from the request Show request | |
| | |
| | |
| Signing | |
| C Greate a self signed certificate with transcerial 1 | |
| Use this Certificate for for signing CaseProva | |
| | |
| | |
| x Signature algorithm SHA 256 ▼ | |
| | |
| | |
| R Templete | |
| Template for the new certificate [[default] CA Apply | |
| | |
| ka Detabase | |
| | |
| Cancel OK | |
| | * |
| | * |
| | • |
| | |
| 🔊 Start 🖉 🛞 🌯 🐊 Jaya - ProvaReti/srctr 💿 X Fertificate and Ke 🗱 KeyTool GUI 1.7 - Ibit 📄 Dibocuments and Sett 🕲 Facebook I Govanni C 🗷 Creare una CA (certific | < 🛒 🛃 🔕 🔧 😭 🛞 🚯 15.35 |

9) Eiminare questa spunta ed assicurarsi che stiamo firmando il certificato appena creato:

10) Andare nel TAB Extension ed anche qui mettere Certification Autority a spuntare la casellina Subject key identifier :

| 🕎 Creare una CA (certification autority).doc - Microsoft Word | _ 8 × |
|---|-----------------------------|
| : Ele Modifica Visualizza Inserisci Figmato Strumenti Izbella Figestra 2 Abber EDF Commenti Acrobat | Digitare una domanda. 🛛 👻 🗙 |
| 🗋 📴 🖟 👌 🗇 🖾 🖓 🇱 🗼 🛍 🖏 🌾 🖤 😕 | |
| 1 Normale Times New Roman 12 G C | |
| L Create x509 Certificate | |
| File Imp: Sance Extensions Key Usage Netscape | |
| Privat Basic dadicare qui | |
| None Type "Certification Extinction Authority Subject Key Identifier | |
| Path length, k. o.: (4) 7 Gritcal Catical Authority Key Identifier | |
| | |
| | |
| | |
| | |
| Validity Time range | |
| Not before 26/05/2009 13:37:16 🚍 Days 💌 | |
| 26/05/2010 9.19.03 🚊 	☐ Midnight | |
| | |
| | |
| | |
| | |
| subject alternative nameEdit | |
| issuer alternative name Edit | |
| CRL distribution point Edit | |
| | L |
| Automory inno Access UC.5P C | |
| Cancel | |
| | ▼ |
| | • |
| | × |
| Disegno + 💫 Eome + 🔪 🔪 💭 📲 🖓 🖉 🖉 🖉 + 🛃 + ☴ 🚍 🛱 🗐 📳 | |
| Pg 5 Sez 1 5/5 A 3,9 cm Ri 4 Col 1 REG REV EST SSC Italiano (Ital 🛄 | |
| 🏦 Start 🏽 🍘 🕲 🧼 📲 Java - ProvaRetijsrcjpr 🛛 🖝 X Certificate and Ke 🐉 Key Tool GUI 1.7 - [D:]] 🔂 D: [Documents and Sett] 😻 Facebook Govanni G] 🛃 Creare una CA (certific. | < 🛒 🔊 🧘 🚱 🎘 🚱 🕅 15.37 |

11) Eseguiamo tutte le procedure come da guida prof.

Poi ritorniamo qui importiamo il CSR appena creato con KeyStore (il csr altro non è che una richiesta di firma di un certificato CERTIFICATION SIGNIN REQUEST) quindi la firmiamo con il certificato di CERTIFICATION AUTORITY creato prima:



12) Quindi lo firmiamo con la nostra certification autority

| 🖳 Creare una CA (certification autority).doc - Microsoft V | tord | |
|--|--|---------------------------|
| Eile Modifica Visualizza Inserisci Formato Strumenti | Iabella Finestra ? Adobe PDF Commenti Acrobat | Digitare una domanda. 🔹 🗙 |
| 🗄 🗅 📂 📕 💪 🚑 i 🖪 💪 i 🌮 🚉 i 🐰 🖿 🛍 🟈 | Service and Key management | |
| A Normale • Times New Roman • 12 • 0 | | |
| L 2 1 . 8-0 | | <u> </u> |
| | Source Extensions Key Usage Netscape Note: Signing request: Signing request: Copy extensions from the request: Signing Create a self signed certificate with the serial 1 Use this Certificate for for signing deade Create a self signed certificate with the serial 1 Use this Certificate for for signing deade Create a self signed certificate with the serial 1 Signature algorithm Signature algorithm Signature algorithm Serial Certificate [[default] CA Cancel Cancel Cancel Cancel Cancel Cancel Cancel Concel Cancel Cancel Concel Ca | × |
| Diseano • 🕞 Forme • 🔪 🔪 🗖 🔿 🖓 🚳 | | // |
| Pa 6 Sez 1 6/6 A 2.4 cm Ri 1 Col 5 | REG REV EST SSC Italiano (Ital D3X | |
| 👔 Start 🥖 🚱 🧶 » 🍃 Java - ProvaReti/src/pr | - X Certificate and Ke 🛐 KeyTool GUI 1.7 - [D:] 🗁 D:]Documents and Sett 🕲 Facebook Giovanni Ci 📄 Creare una CA (certific 🔍 | < 🕵 🖻 🙆 🦹 💽 🎅 🗞 15.47 |
| | | |

Dobbiamo solo scegliere cosa firmare e con cosa frmarlo non dobbiamo cambiare niente altro.

13) come si puo ossrevare nella pagina certificate abbiamo sotto GuidaProva il nostro certificato firmato, GuidaProva è la nostra CA che ha firmatoGuidaKey

| 🖳 Creare una CA (certification autority). | .doc - Microsoft Word | X |
|---|--|-----------------------------|
| Eile Modifica Visualizza Inserisci Fo | grmato Strumenti Iabella Figestra 2 Adobe PDF Commenti Acrobat | Digitare una domanda. 🛛 👻 🗙 |
| i 🗅 💕 🖬 🖪 🖨 🖪 🖪 🖉 🖏 i | X 🐚 🔁 🍼 • 🔍 - 🧐 🐺 📰 🖓 🏭 🗱 🗱 🐼 🔍 🖤 100% - • @ 💷 Lettura 📑 🔁 🔁 💨 📑 | |
| Mormale - Times New Roman | • 12 • G C S 圖書書畫 詞 • 詞 : 語 : 編 : - 詞 • ¹⁰ • <u>A</u> •] | |
| L | 2 1 S-X Certificate and Key management | - - |
| | File Import Help | |
| | Private Keys Certificate signing requests Certificates Templates Revocation lists | |
| N. | Internal name ∇ Common name Serial not After Trust state B New Certificate New Certificate | |
| - - - | Rischiesta Rischiesta 02 2010-05 Trust inheriter Export | |
| - - - | Client Client 02 2010-05 Trust inheriter | |
| | 🗗 💓 GuidaProva 01 2010-05 Always Truste Show Details | |
| • •• | Delete | |
| | GuidaKey GuidaKey 02 2010-05 Trust inheriter Import PKCS#12 | |
| - | Import PKCS#7 | |
| - | Plain View | |
| - 4 | | |
| | | |
| - | Dunbach 7 in | |
| - | | |
| - | | |
| | Databasen'n' Don mente and Settings (Viller/Deckton/databaseliev vdb | |
| | | |
| - | [mage: 2][pose: / / / □ ○ □ 通 ① 司 □ ○ - ▲ - ▲ - 田 井 幸 句 ■ ■ ● 国 > □ □ □ □ ■ ● ○ □ ■ ● ○ □ ■ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● | • |
| | Fry S. Sei L. SS. A. H. Col. HELER (2013) Baker (2014) 🔟 🖾 State (2014) Col. State (2014) Col. Stat | * |
| | | Ŧ |
| Disegno + 🔓 Eorme + 🔪 🔪 🗆 🔿 | | |
| Pg 6 Sez 1 6/6 A 2,4 cm | m Ri 1 Col 2 REG REV EST SSC Italiano (Ital | |
| 🍂 Start 🛛 🏉 🚱 🧶 🔹 🍃 Java - Pro | waReti/src/pr 🗫 X Certificate and Ke 🔰 KeyTool GUI 1.7 - [D:\ 🗁 D:\Documents and Sett 🧐 Facebook Giovanni G 🖃 Creare una CA (certific. | 🔍 🛒 🙆 🦹 🙆 👰 🗞 15.44 |

Giovanni Cirelli