

HTTPS e Certificati SSL

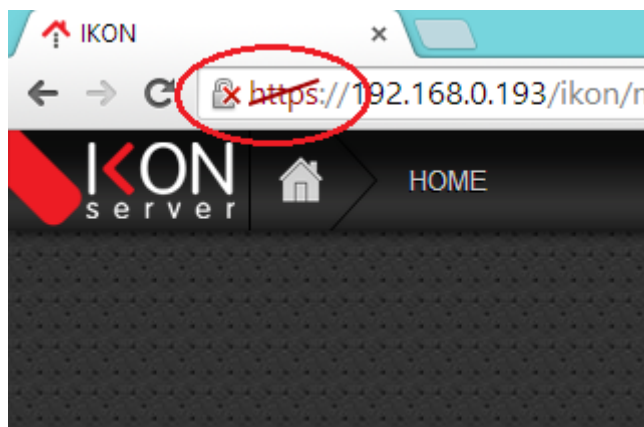
Configurare Certificati SSL

Dalla versione **1.3.0** in poi, iKon è in grado di generare certificati SSL corretti per un accesso più sicuro. Per poter sfruttare appieno questa nuova funzionalità, è necessario effettuare una breve operazione su ciascun client che desidera accedere ai prodotti [Domotica Labs](#).

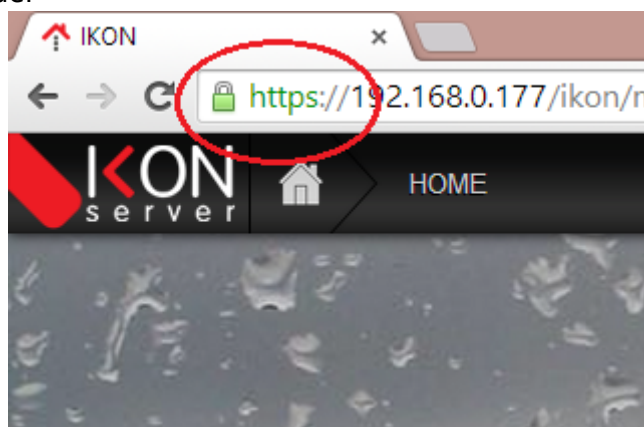
L'operazione è molto semplice, differisce leggermente a seconda del sistema operativo che si sta usando e consiste semplicemente nell'indicare [Domotica Labs](#) come una sorgente affidabile di certificati SSL sia sul browser che su Java.

Tale configurazione deve esser eseguita **una sola volta** su ciascuna macchina che si desidera usare con i prodotti [Domotica Labs](#)

Se un client non è configurato, accedendo ad un iKon in HTTPS, in alto a sinistra nella barra degli indirizzi verrà mostrato un lucchetto "aperto" e verranno continuamente mostrati dei messaggi di "Warning" ad ogni accesso.



In caso contrario, se il client considera [Domotica Labs](#) come una sorgente affidabile di certificati, si mostrerà un lucchetto verde.

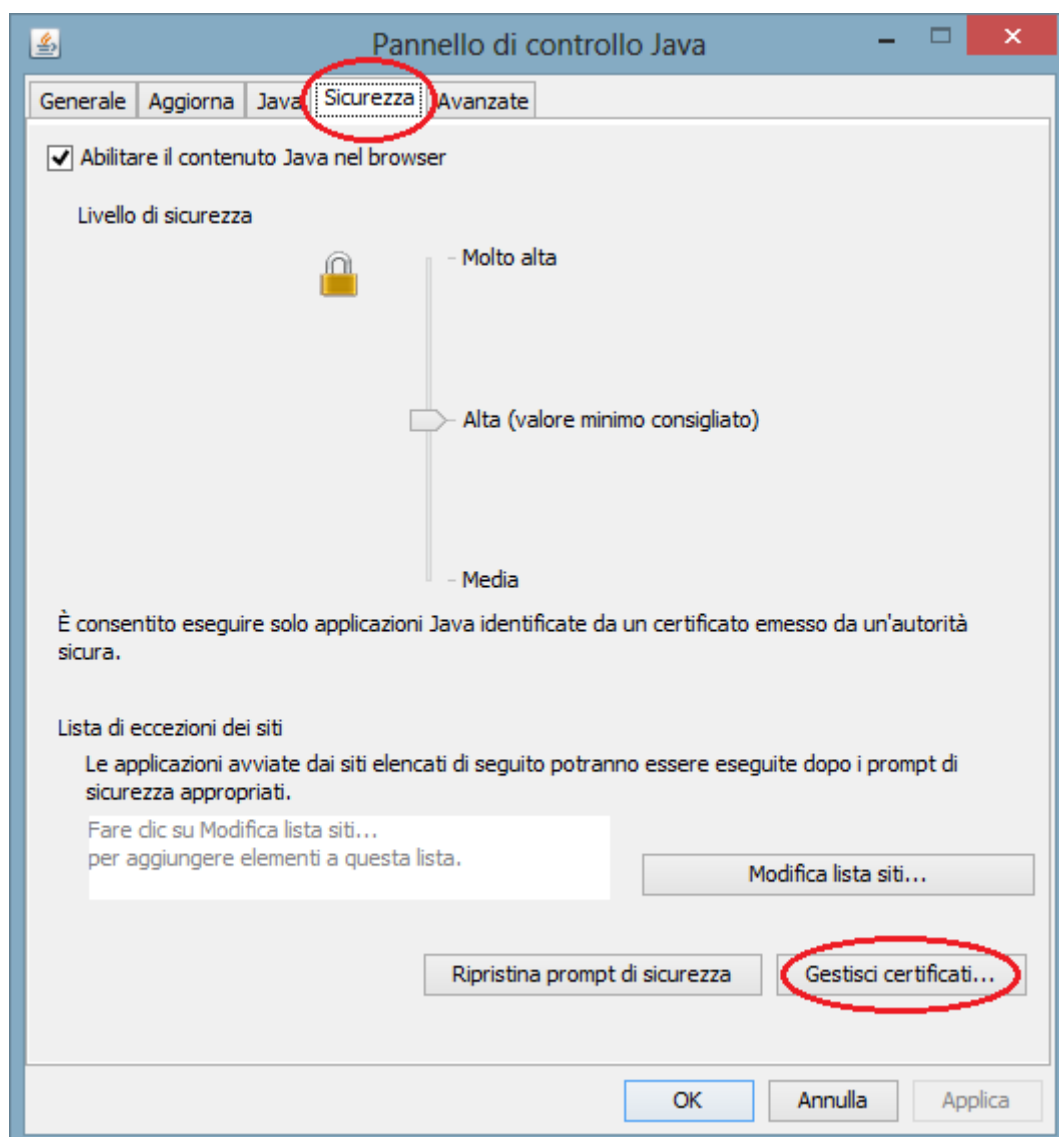


Per configurare [Domotica Labs](#) come una sorgente affidabile di certificati è sufficiente effettuare le seguenti operazioni:

Java

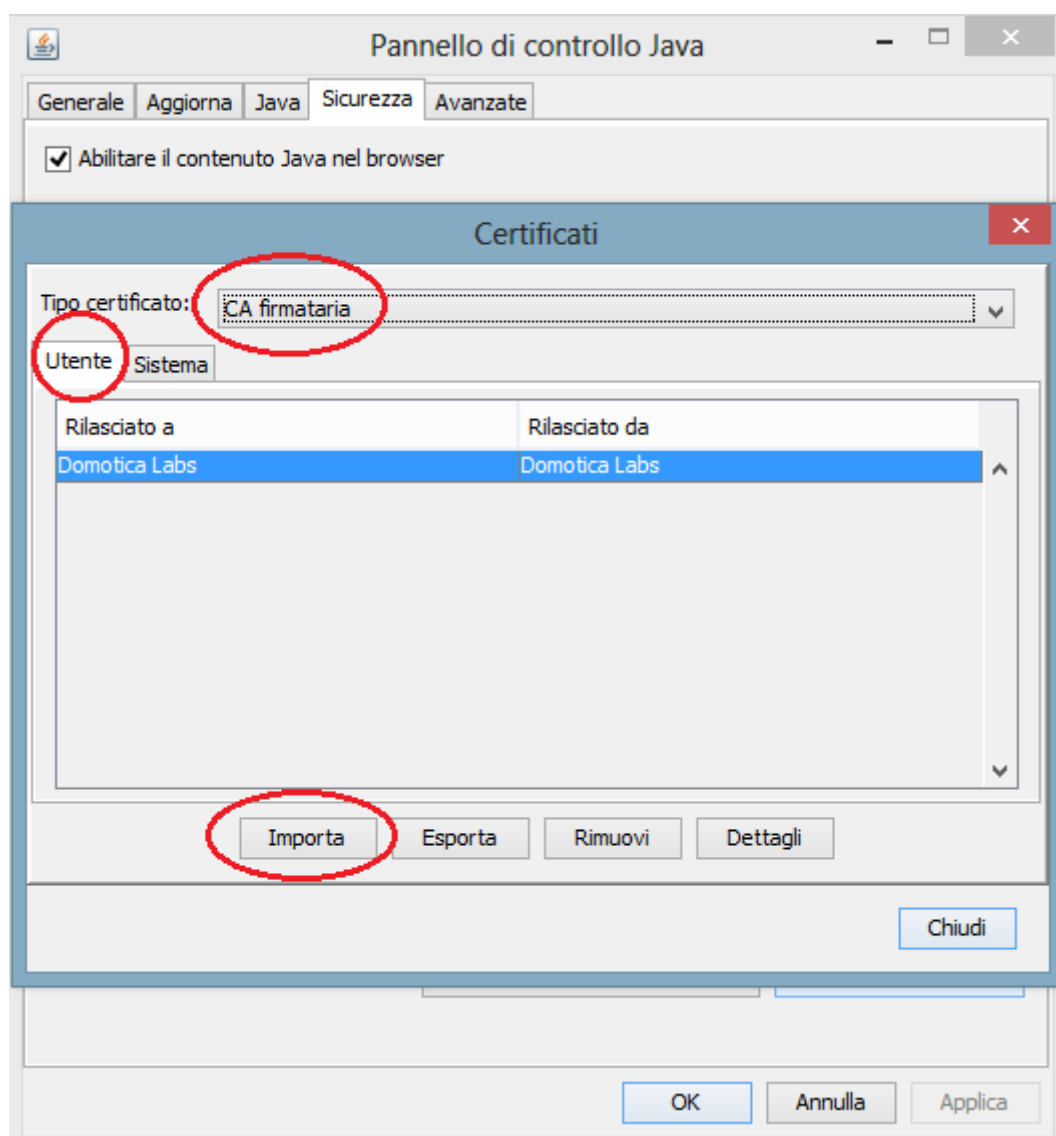
Questa operazione è necessaria solo se si desidera accedere in HTTPS ad iKon con il modulo **VoIP licenziato**, ed evitare messaggi di “warning” generati da Java.

- Scaricare il certificato di CA (Certification Authority) di [Domotica Labs](#) dal seguente indirizzo: [certificato CA](#).
- Avviare il “Pannello di Controllo Java”, selezionare l'etichetta “Sicurezza” e premere il bottone “Gestisci Certificati”



- Selezionare la linguetta “Utente”

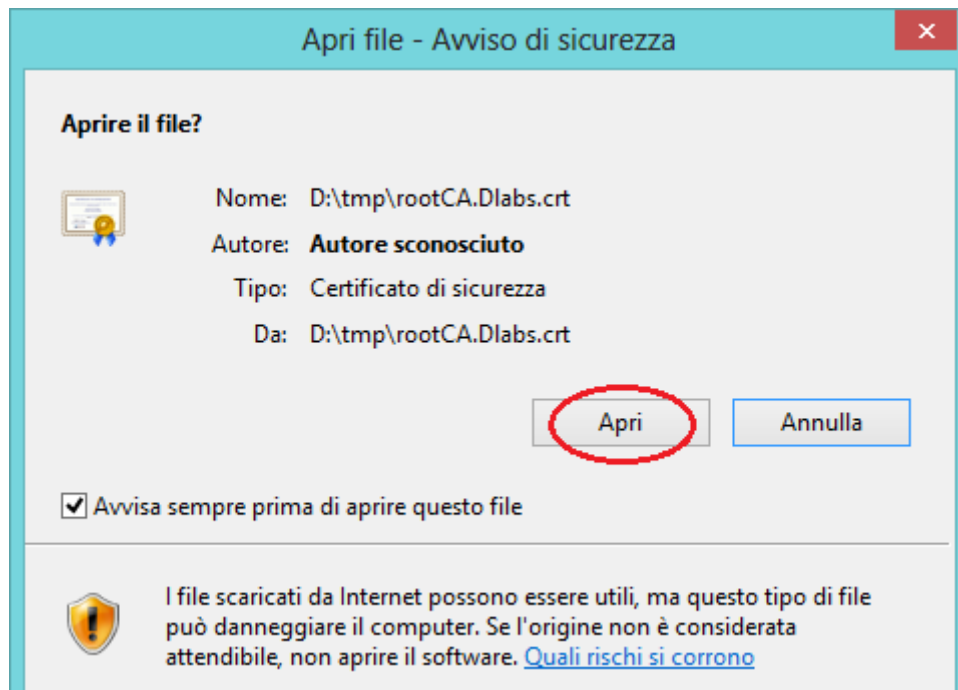
- Selezionare il Tipo di certificato “CA Firmataria”
- Premere il bottone “Importa”



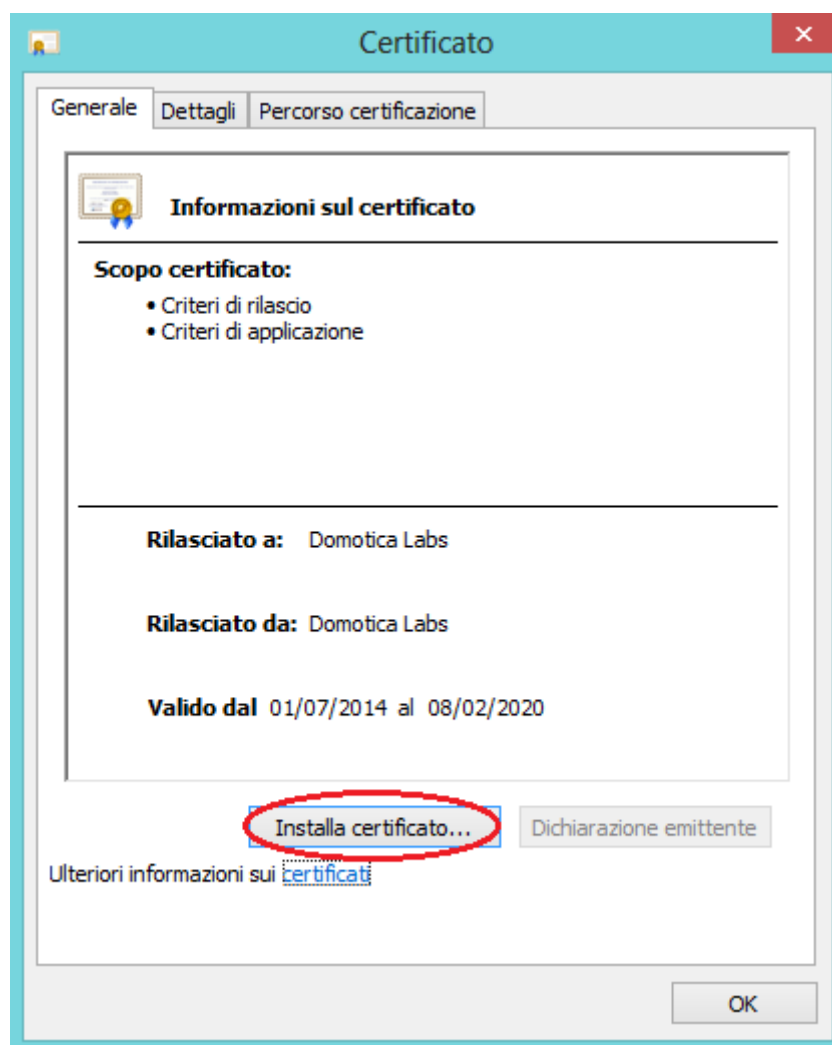
- Selezionare il file [certificato CA](#) appena scaricato.
- Ripete l'operazione per tutti gli utenti della macchina coinvolti dall'uso della domotica

Windows - Chrome e IE

- Rammentare che IE non è ufficialmente supportato. Nulla vieta tuttavia di provare ad utilizzarlo per navigare un iKon configurato con Chrome.
- Accedere a Windows con un utente di amministrazione.
- Scaricare il certificato di CA (Certification Authority) di [Domotica Labs](#) dal seguente indirizzo: [certificato CA](#).
- Fare un doppio-click sul file scaricato.
- Concedere al sistema di aprire il file nel caso si presenti un messaggio di warning.

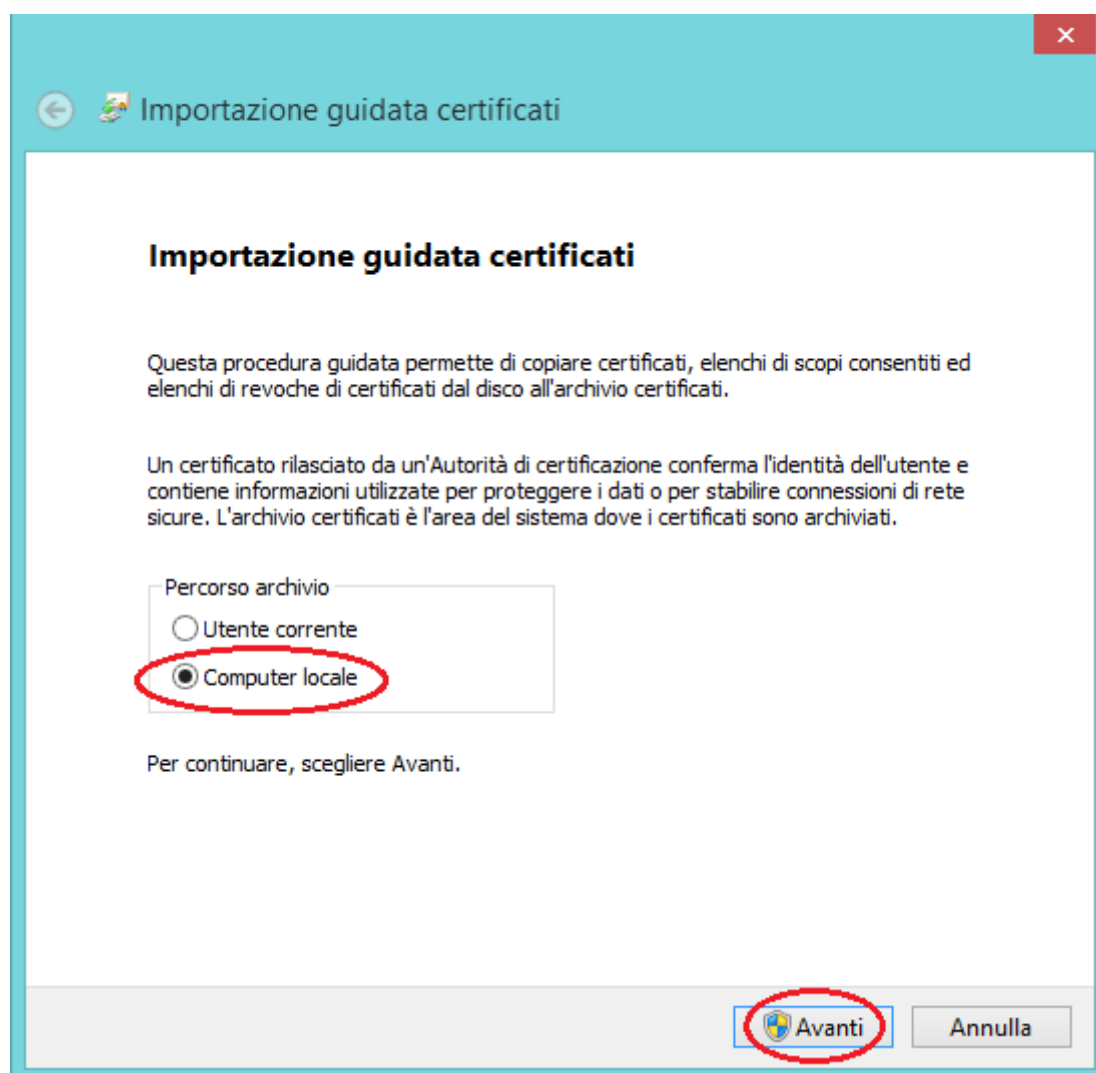


- Premere sul pulsante "Installa certificato".

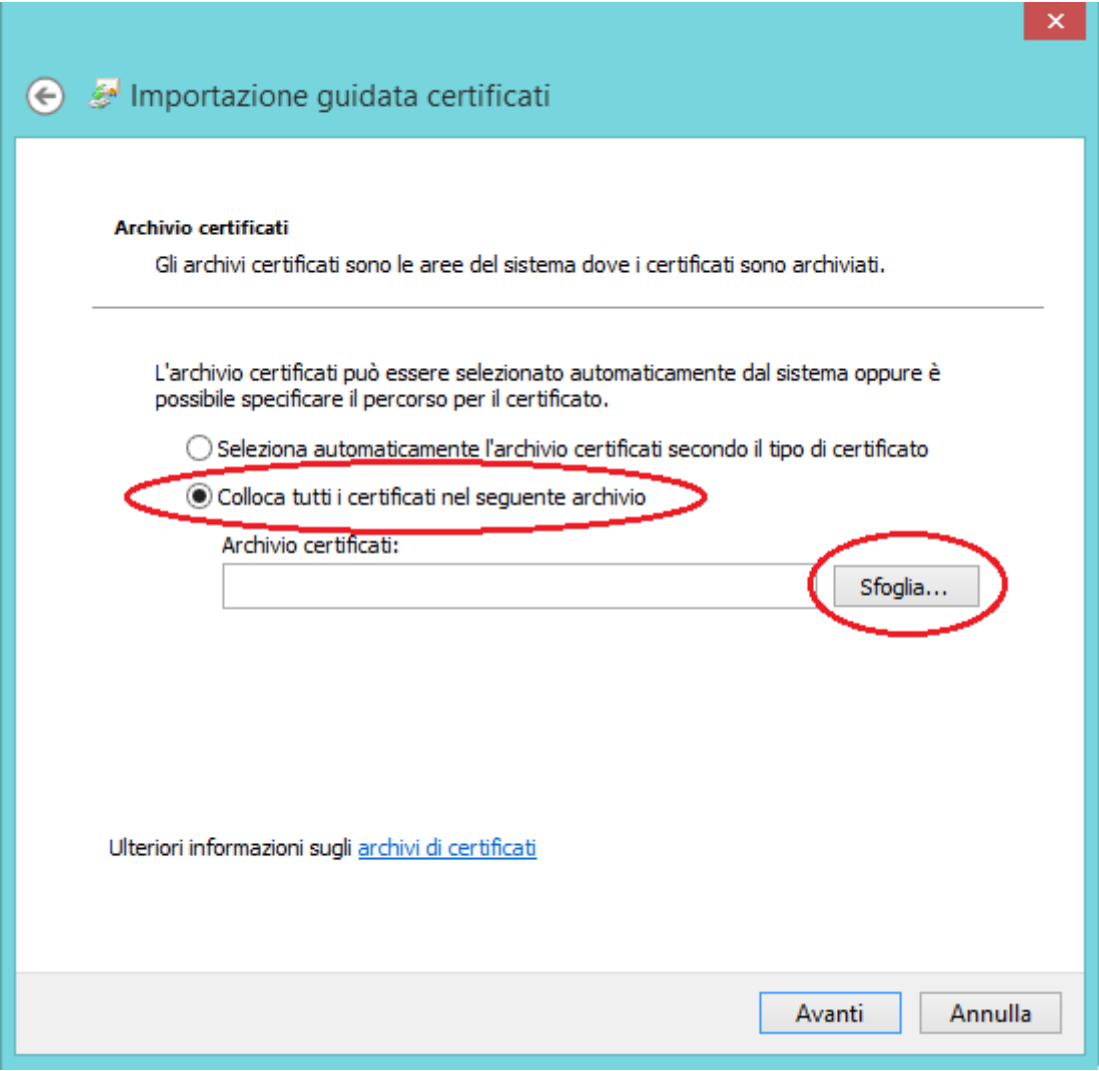


- Selezionare di voler installare il certificato sul "Computer Locale" (nulla vieta di installare il certificato solo sull'utente corrente; tuttavia deve esser chiaro che, accedendo con un utente

differente, Windows non considererà più [Domotica Labs](#) come una sorgente affidabile di certificati) e poi premere “Avanti”.



- Selezionare di voler collocare il certificato in un archivio specifico e poi premere “Sfogliare”.



Importazione guidata certificati

Archivio certificati

Gli archivi certificati sono le aree del sistema dove i certificati sono archiviati.

L'archivio certificati può essere selezionato automaticamente dal sistema oppure è possibile specificare il percorso per il certificato.

☐ Seleziona automaticamente l'archivio certificati secondo il tipo di certificato

☒ Colloca tutti i certificati nel seguente archivio

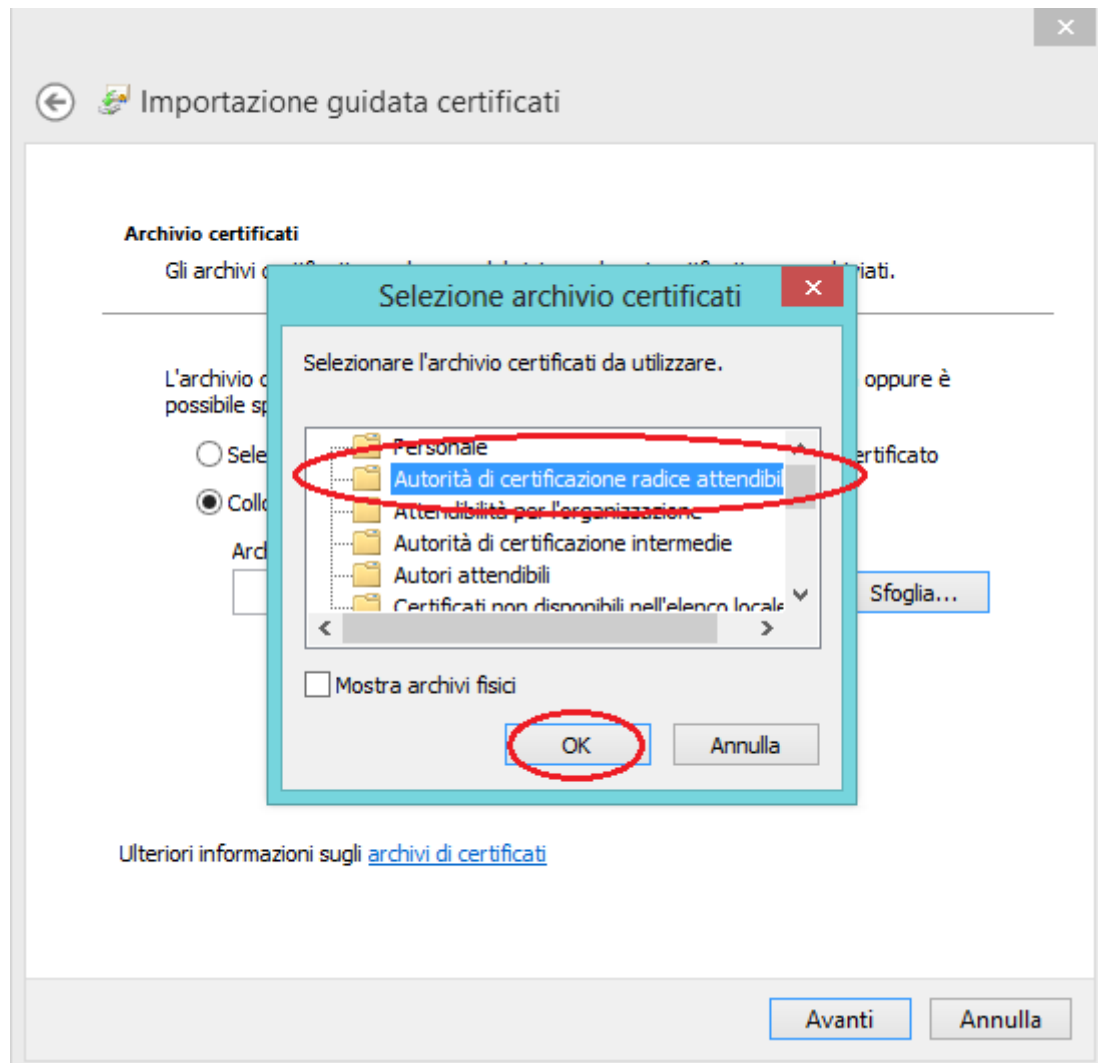
Archivio certificati:

Sfogli...

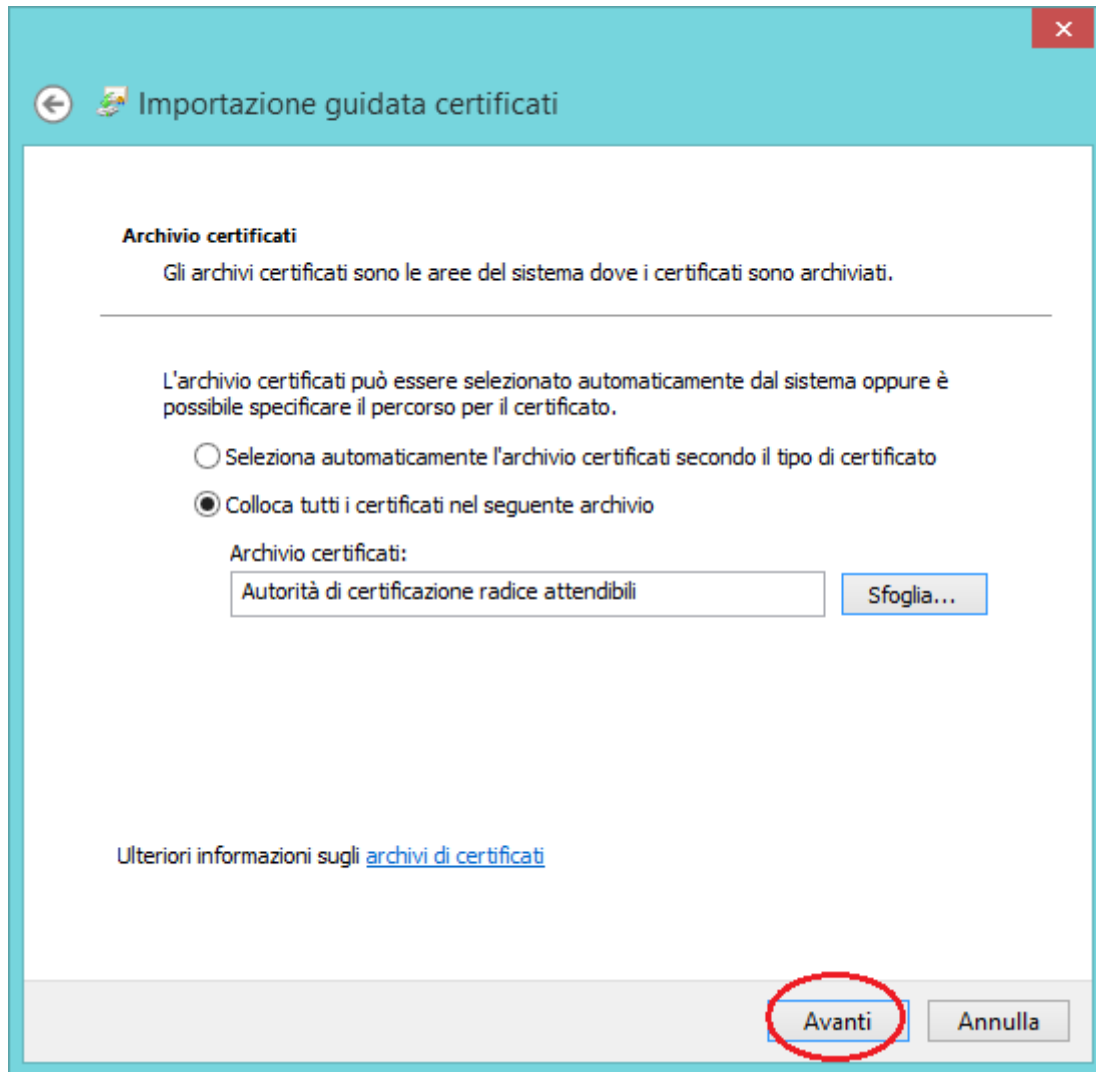
Ulteriori informazioni sugli [archivi di certificati](#)

Avanti Annulla

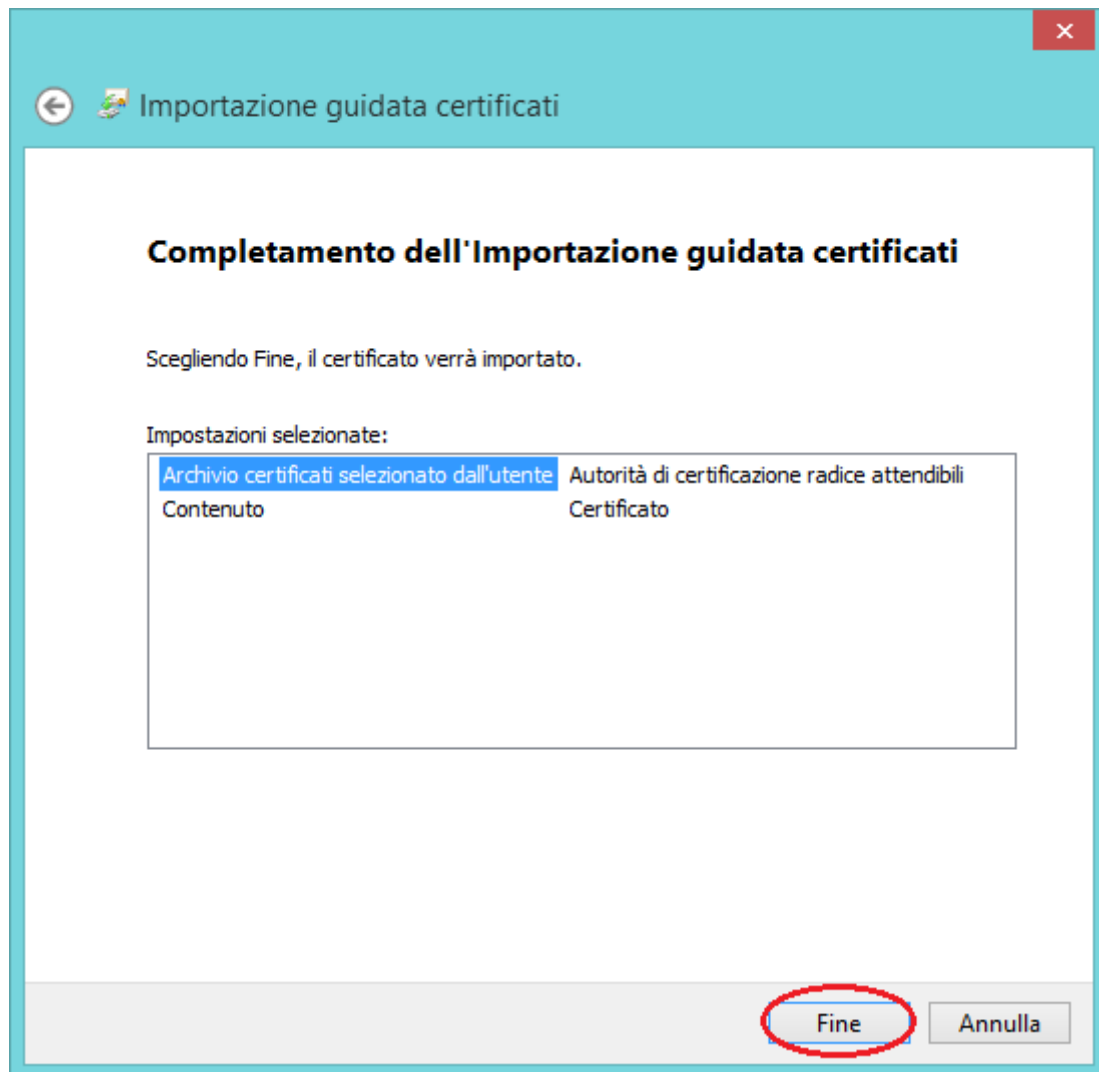
- Selezionare l'archivio "Autorità di certificazione di radice attendibile" e poi premere "Ok".



- Dopodichè premere "Avanti".

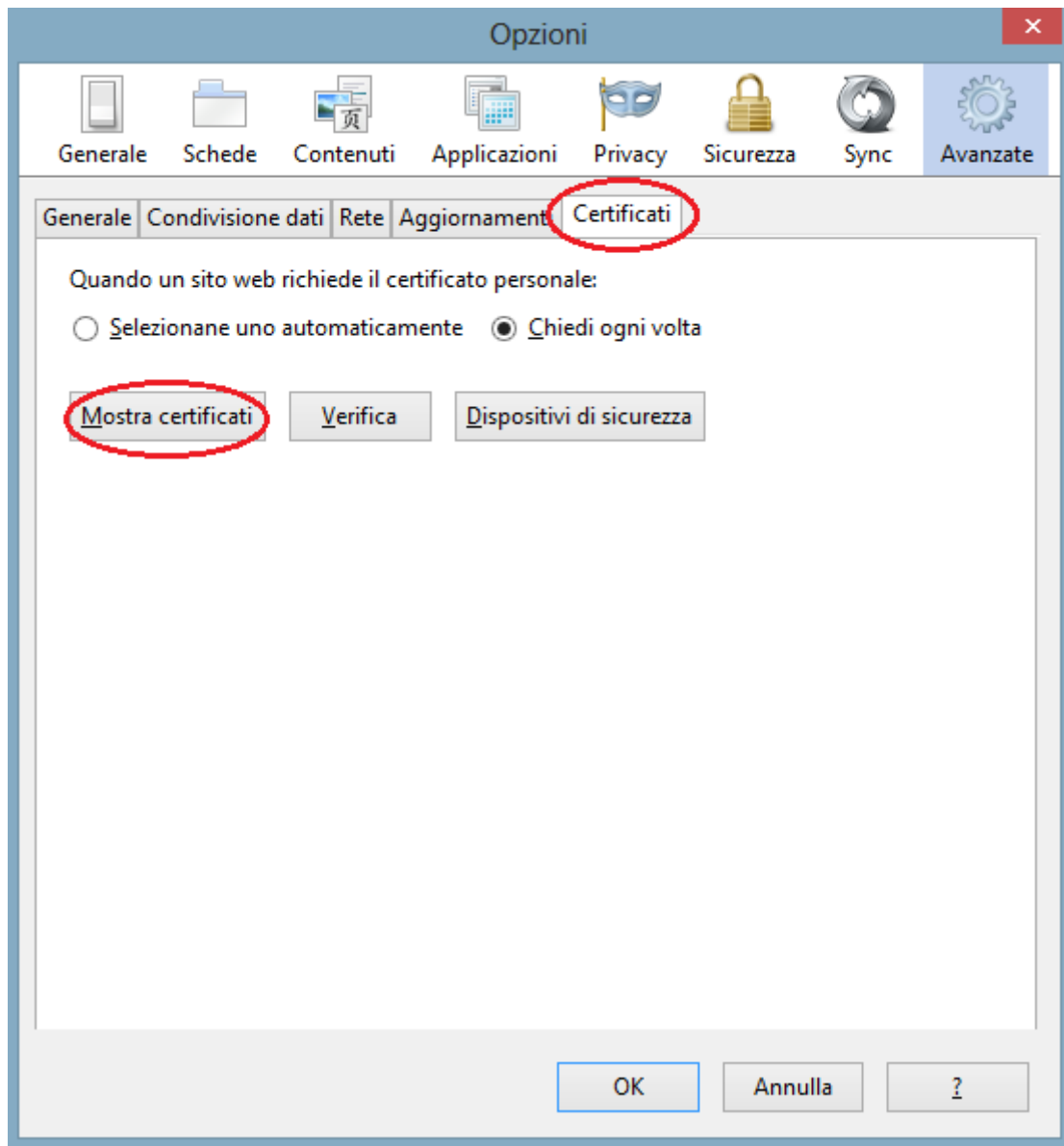


- Premere "Fine" per completare l'installazione.

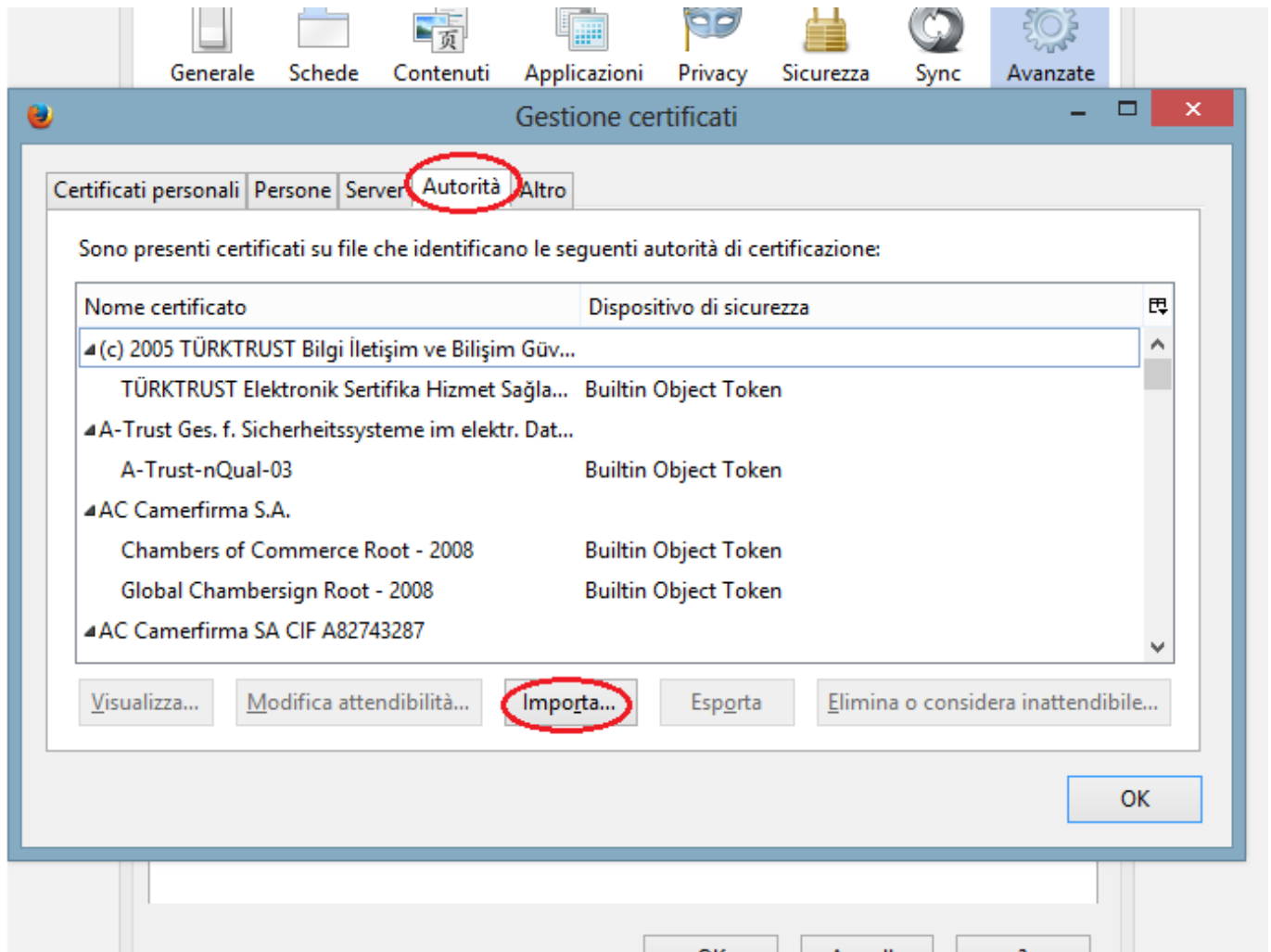


Windows - Firefox

- Rammentare che Firefox non è ufficialmente supportato. Nulla vieta tuttavia di provare ad utilizzarlo per navigare un iKon configurato con Chrome.
- Scaricare il certificato di CA (Certification Authority) di [Domotica Labs](#) dal seguente indirizzo: [certificato CA](#).
- Accedere alle "Opzioni" di Firefox dal menù principale del browser
- Premere sull'etichetta "Certificati" e poi su "Mostra Certificati"



- Premere su "Autorità" e poi su "Importa"



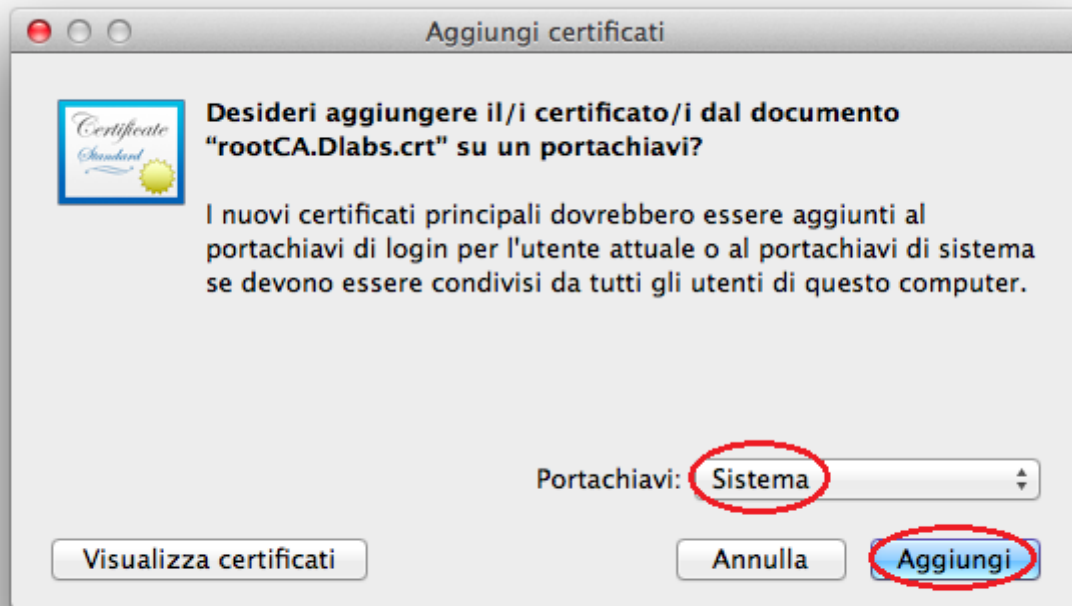
- Selezionare il certificato di CA di [Domotica Labs](#) appena scaricato.
- Al termine dell'operazione, nella lista dei certificati delle "Autorit" apparir la voce [Domotica Labs](#)

Windows XP o Windows 2000 o Windows 7 Embedded - Chrome e IE

Usare Microsoft Management Console (MMC) (Vedi [tutorial](#).)

Apple MAC

- Scaricare il certificato di CA (Certification Authority) di [Domotica Labs](#) dal seguente indirizzo: [certificato CA](#).
- Fare doppio click sul certificato appena scaricato
- Aggiungere il certificato al portachiavi di "Sistema" (nulla vieta di installare il certificato solo al portachiavi di "login"; tuttavia deve esser chiaro che, accedendo con un utente differente, Windows non considerer pi [Domotica Labs](#) come una sorgente affidabile di certificati)



Apple iPhone/iPad

Metodo 1

- Aprire Safari sul dispositivo su cui si vuole installare il certificato
- Inserire l'indirizzo relativo al [certificato CA](#)
- Sul dispositivo si aprirà una finestra di conferma come la seguente

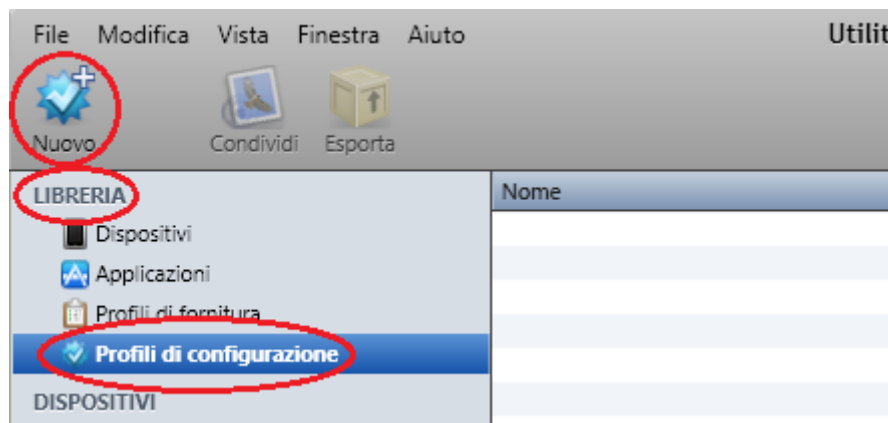


- Cliccare sul pulsante in alto a destra "Installa" e si aprirà una ulteriore schermata di conferma
- Cliccare di nuovo sul pulsante "Installa"
- A questo punto il certificato è installato e dovreste vedere una schermata con una spunta verde, come la seguente
- Cliccare sul pulsante "Fine" per terminare la procedura

NB: una volta installato il certificato è buona norma chiudere tutti browser (anche dal background), fare una pulizia delle cache e riavviarli.

Metodo 2

- Scaricare, se necessario, il software [iPhone configuration utility](#)
- Scaricare il certificato di CA (Certification Authority) di [Domotica Labs](#) dal seguente indirizzo: [certificato CA](#).
- Avviare [iPhone configuration utility](#)
- Sotto la voce "Libreria", selezionare "Profili di configurazione"



- Scegli se creare o importare un profilo di configurazione:
 - **Importa** profilo esistente (soluzione base):
 - Scaricare il seguente [profilo pregenerato](#) e scompattarlo.
 - Premere "File", poi "Aggiungi alla libreria" e selezionare il profilo appena scaricato e scompattato.
 - **Nuovo** profilo di configurazione (soluzione avanzata):
 - premere "Nuovo" in alto a sinistra
 - Sotto "Generale" riempire i dati obbligatori
 - Sotto "Credenziali" aggiungere il [certificato CA](#) di [Domotica Labs](#)
- Connettere **fisicamente** iPhone al PC/MAC
- Selezione il tuo iPhone/iPad nella sezione "Dispositivi" e poi seleziona la linguetta "Profili di configurazione"; infine premi il pulsante "Installa" accanto al profilo di configurazione appena creato/importato.



- Sul dispositivo iPhone/iPad apparirà una finestra di conferma; premi il bottone “installa” e segui la procedura premendo i pulsanti “installa”.



- Al termine della procedura verrà mostrato il certificato installato



Android Mobile

Per poter installare un certificato su un qualsiasi dispositivo Android è necessario aver configurato almeno un a protezione al dispositivo (ad esempio: il PIN). Nel caso non si sia configurata alcuna protezione il dispositivo Android richiederà prima di configurarla.

- Accedere con il browser all'indirizzo: [certificato CA](#).
- Accettare di voler installare il certificato e seguire la procedura descritta dal dispositivo.

UNIX Debian

- Scaricare il certificato di CA (Certification Authority) di [Domotica Labs](#) dal seguente indirizzo: [certificato CA](#).
- Eseguire i seguenti comandi:

```
apt-get install libnss3-tools
```

```
certutil -d sql:/mnt/storage/RWdlabs/guest/.pki/nssdb -A -t TC -n  
"rootCA.Dlabs" -i rootCA.Dlabs.crt
```

```
sudo mkdir /usr/share/ca-certificates/extra
```

```
sudo cp foo.crt /usr/share/ca-certificates/extra/foo.crt
```

```
sudo dpkg-reconfigure ca-certificates
```

Configurare dominio di accesso remoto

Se si desidera accedere ai prodotti [Domotica Labs](#) in HTTPS da remoto, è necessario anche configurare il “**Dominio di accesso remoto**” nella pagina di configurazione di “**Rete**”.

Il dominio è quella parte compresa tra il protocollo e la porta di accesso.

Ad esempio: se l'accesso da remoto è “*https:example.dyndns.org:4123*” il dominio di accesso remoto è: “**example.dyndns.org**”

Rigenerare Certificati SSL

Ogni prodotto [Domotica Labs](#), provvede a rigenerare automaticamente, in piena autonomia, i certificati per l'accesso HTTPS.

I certificati vengono rigenerati **solo** se il prodotto ha **accesso ad internet**. In caso contrario l'operazione termina senza errori ma non produce alcun risultato lasciando i certificati originali intatti.

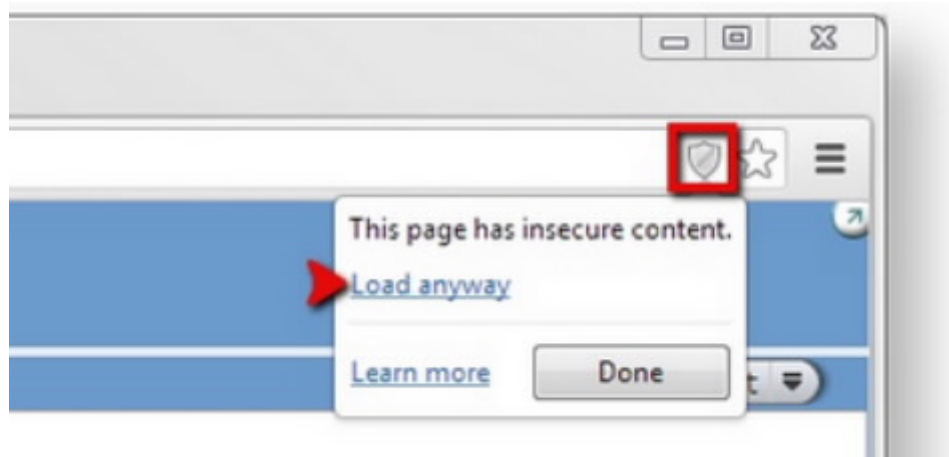
La rigenerazione dei certificati avviene quando:

- Viene **aggiornato il software**
- Viene configurato un **nuovo IP**
- Viene configurato un **nuovo dominio di accesso** remoto
- Viene utilizzato il pulsante “**Rigenera certificati**” sotto il menù di “sistema” → “manutenzione”

Nel caso si rigenerino i certificati a mano attraverso il menù di **manutenzione**, è necessario premere il pulsante “**Riavvi servizi Web**” dopo l'operazione di rigenerazione.

Non si vedono alcuni contenuti

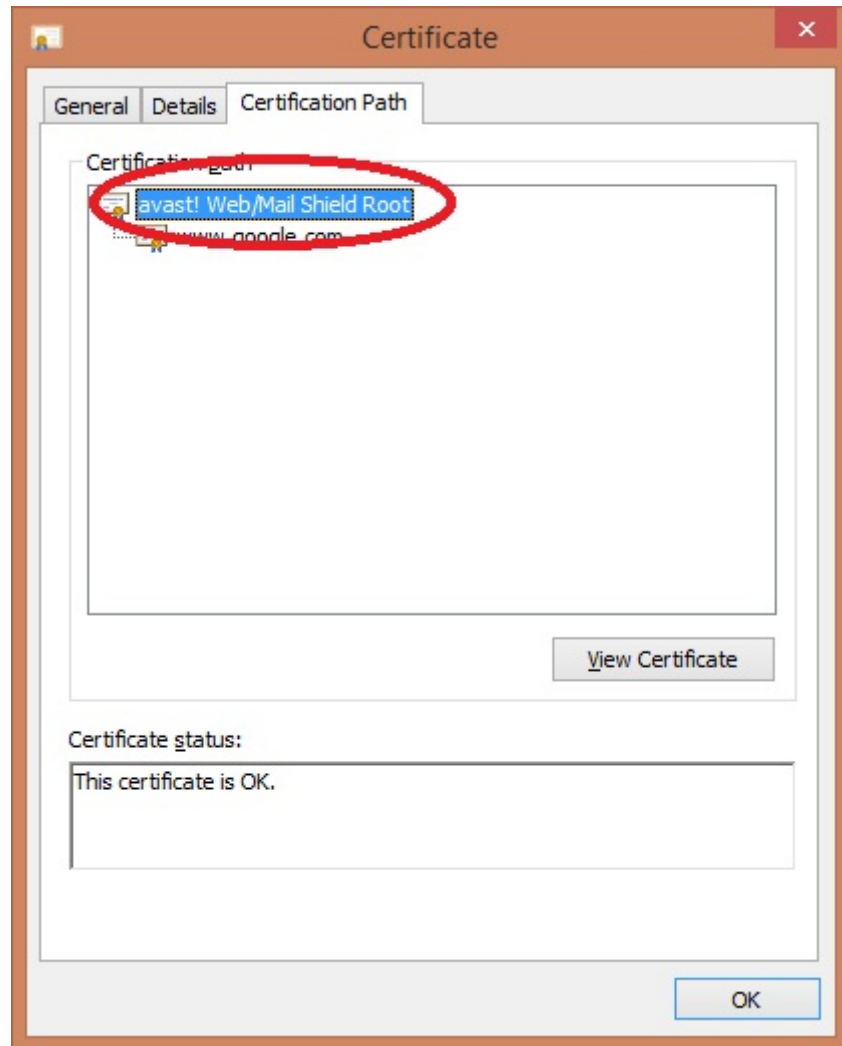
Quando si accede in HTTPS è possibile che non si riescano a vedere contenuti di rete non sicuri a cui iKon accede in HTTP (Ad esempio: le telecamere locali). Su chrome è necessario sbloccare il lucchetto in alto a destra nella barra degli indirizzi:



Avast 2015

Avast 2015, attraverso il servizio "Mail Shield", tende ad intromettersi nel sistema di certificazione SSL e decide, in piena autonomia, che i certificati Domotica Labs non sono attendibili. Questo significa che, anche se si è configurato correttamente tutto, il "lucchetto" della pagina web in HTTPS rimane comunque "rosso".

Per controllare se Avast si sta intromettendo nel sistema basta premere sul pulsante del "Lucchetto" e confrontarlo con il seguente screenshot:



Le soluzioni sono le seguenti:

- Disattivare il "Mail Shield" di Avast 2015
- Disattivare la configurazione "esamina traffico di rete crittografato SSL" andando in: Protezione esplorazione WEB → ONLINE SHIELD → IMPOSTAZIONE AVANZATA.

From:
<http://www.domoticalabs.com/dokuwiki/> - **DOMOTICA LABS WIKI**

Permanent link:
<http://www.domoticalabs.com/dokuwiki/doku.php?id=ikon:faqs:network:ssl:ssl&rev=1426072063>

Last update: **2015/03/11 11:07**