DOCUMENTAZIONE FIREBIRD

FLASHINLABS S.N.C. Piazza del mercato 9, 50032 Borgo san Lorenzo (FI)

SOMMARIO

INTRODUZIONE

Il sistema Firebird consente la regolamentazione dell'accesso ad Internet di una o più reti interne.

Il sistema prevede l'interfacciamento ai sistemi di Google per l'autenticazione e la discriminazione del tipo di accesso ad Internet.

Per ottenere questa funzionalità, il sistema si serve di due componenti principali: un server e un firewall.

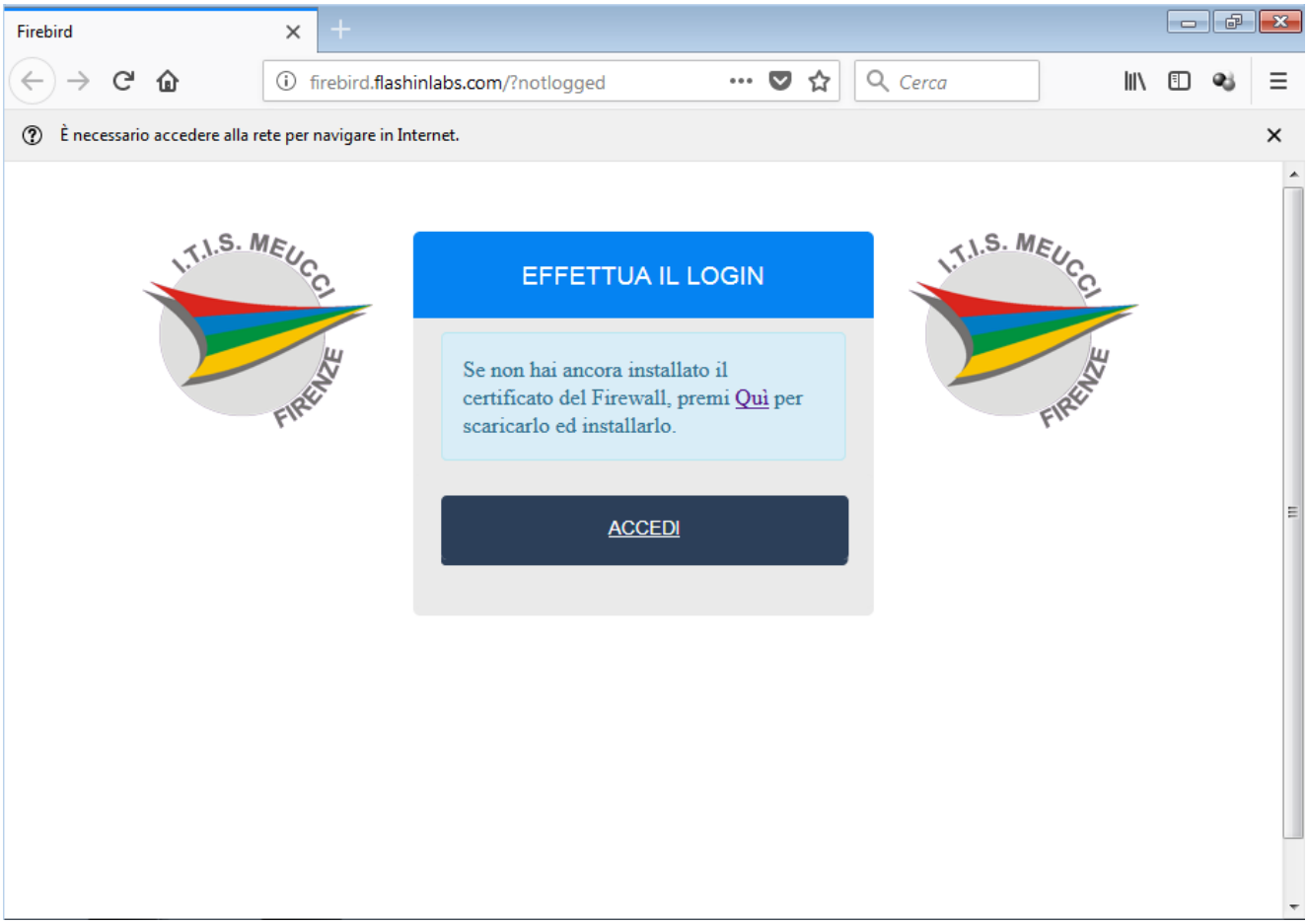
Il server viene utilizzato per le funzionalità di logging e accounting, mentre il firewall gestisce le connessioni wan e le varie vlan di accesso.

UTILIZZO LATO CLIENT

I pc connessi alle reti gestite da Firebird non avranno accesso ad Internet automaticamente; sarà infatti necessario eseguire il Login.

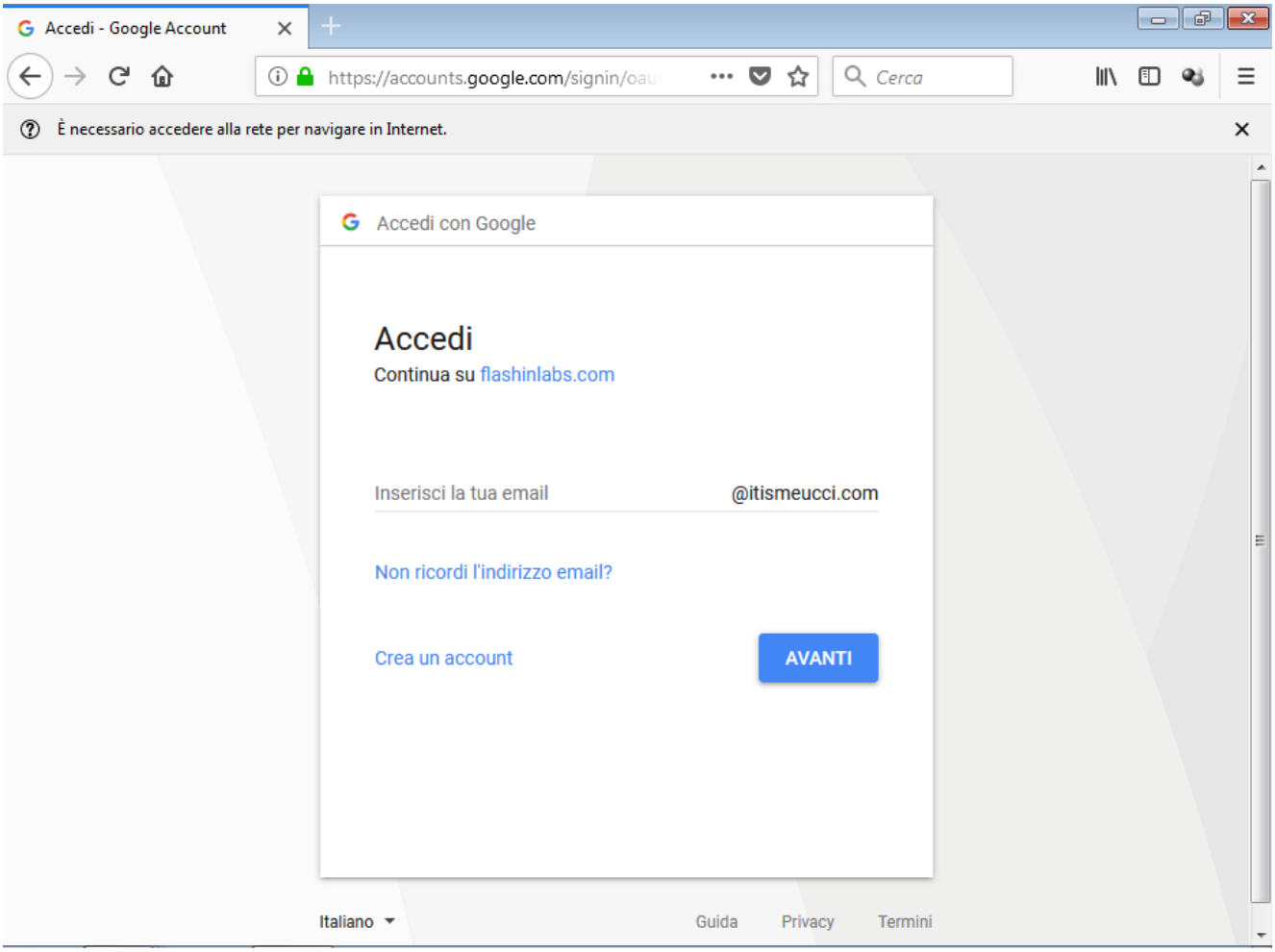
Per eseguire il login è sufficiente navigare all'indirizzo http://firebird.flashinlabs.com oppure navigare su un qualsiasi sito internet; il browser verrà quindi ridiretto alla pagina di login.

Segue un esempio di pagina di Login

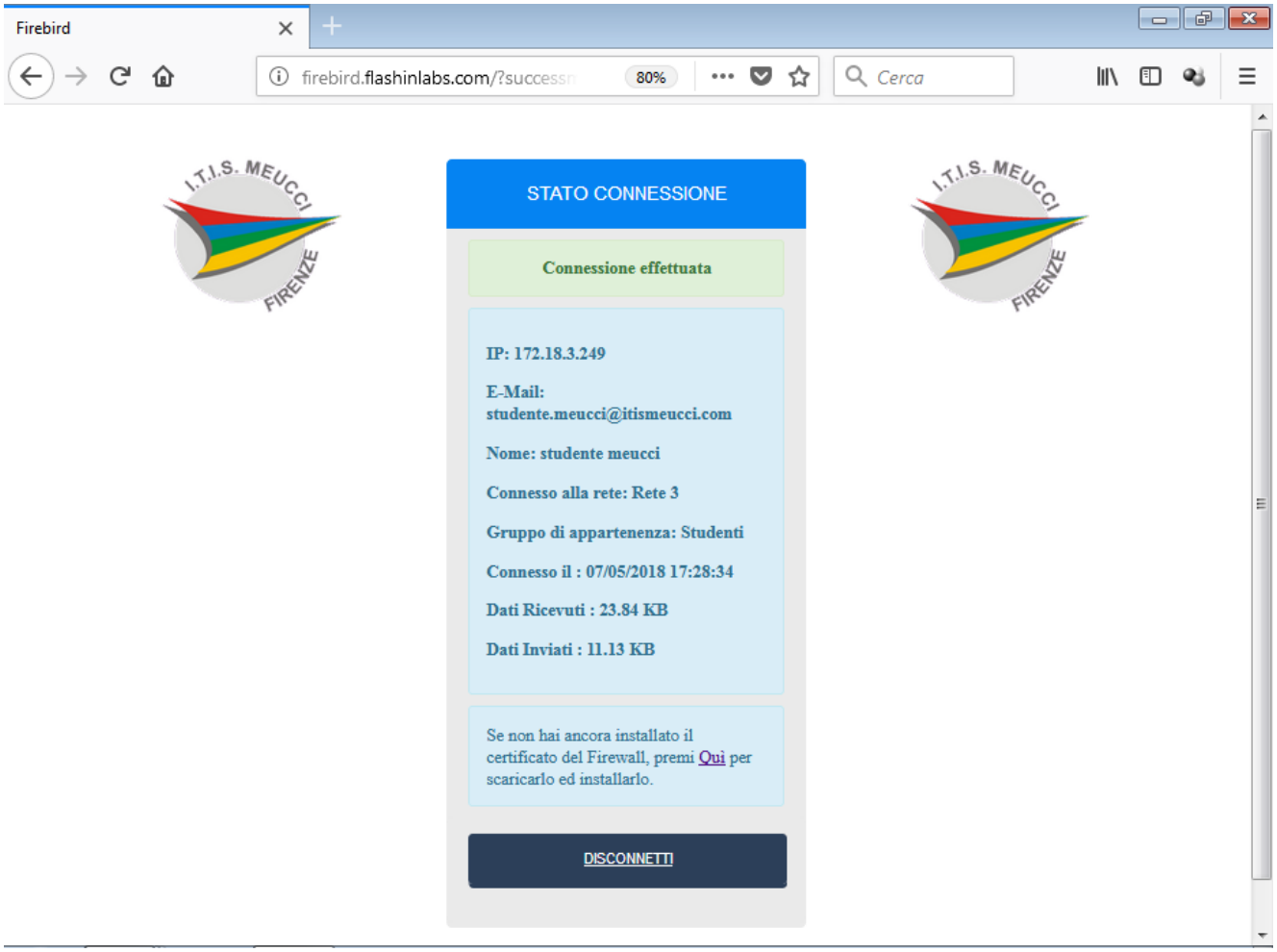


Cliccando sul tasto Accedi veniamo ridiretti sul pannello di Login di Google, così da poter inserire le credenziali.

Nota: Il sistema permette il login soltanto utilizzando credenziali @**itismeucci.com.**



Una volta inserita la propria mail e la propria password la procedura di Login termina e viene presentato il pannello di stato.



Questa schermata, sempre raggiungibile tramite l'url http://firebird.flashinlabs.com, mostra lo stato della connessione. È presente il tasto "Disconnetti" per effettuare la disconnessione esplicita.

INSTALLAZIONE CERTIFICATO

Informazioni generali

Il sistema, per permettere il filtro dei contenuti, effettua una ispezione del traffico.

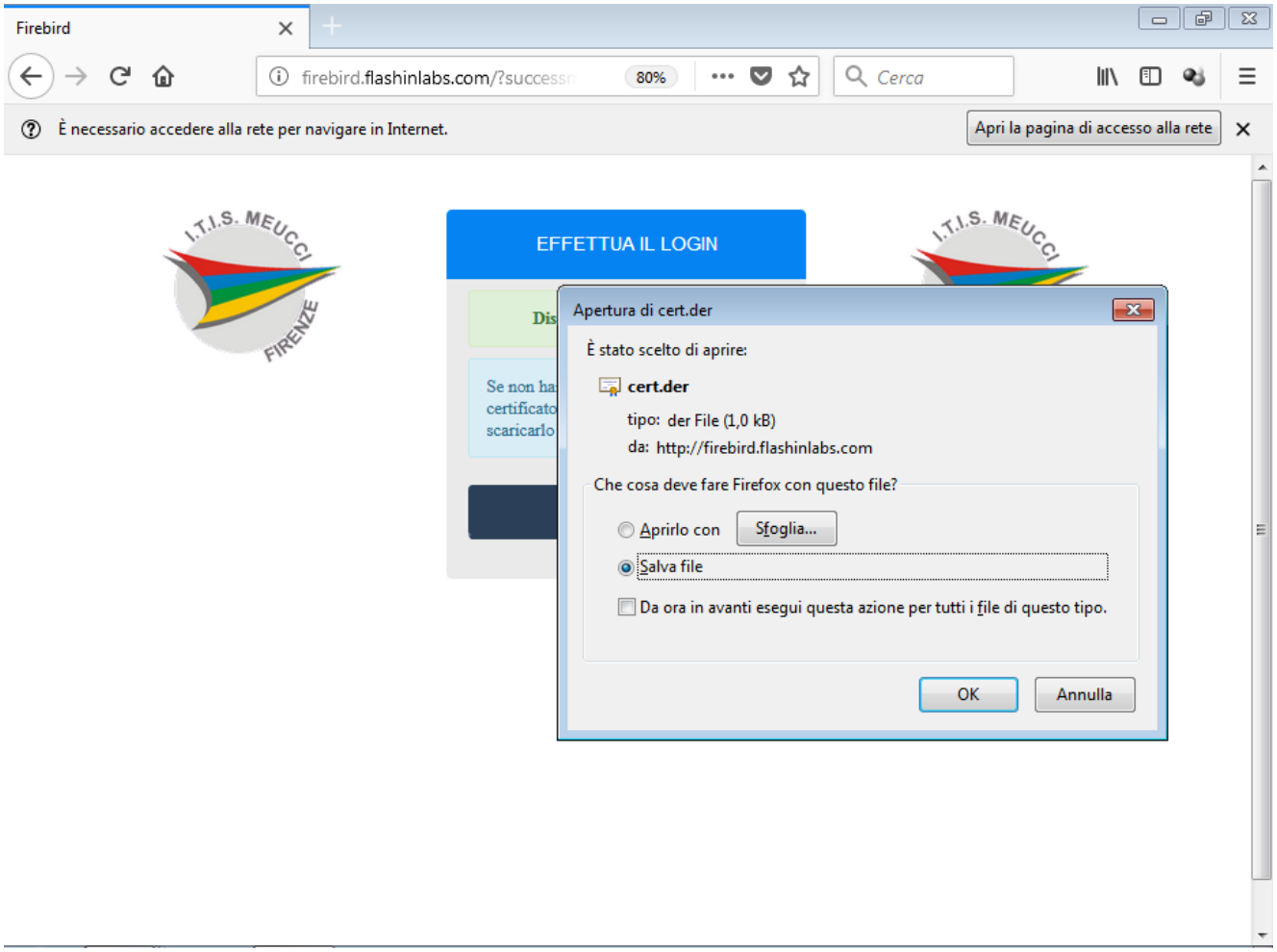
L'ispezione avviene anche sulla porta 443, quindi sul traffico tramite protocollo HTTPS.

Questo comporta la necessità di installare, su tutti i dispositivi utilizzati per la navigazione, di un certificato radice attendibile (CA Certificate).

Il certificato è scaricabile direttamente dalla schermata di login.

Installazione su Firefox

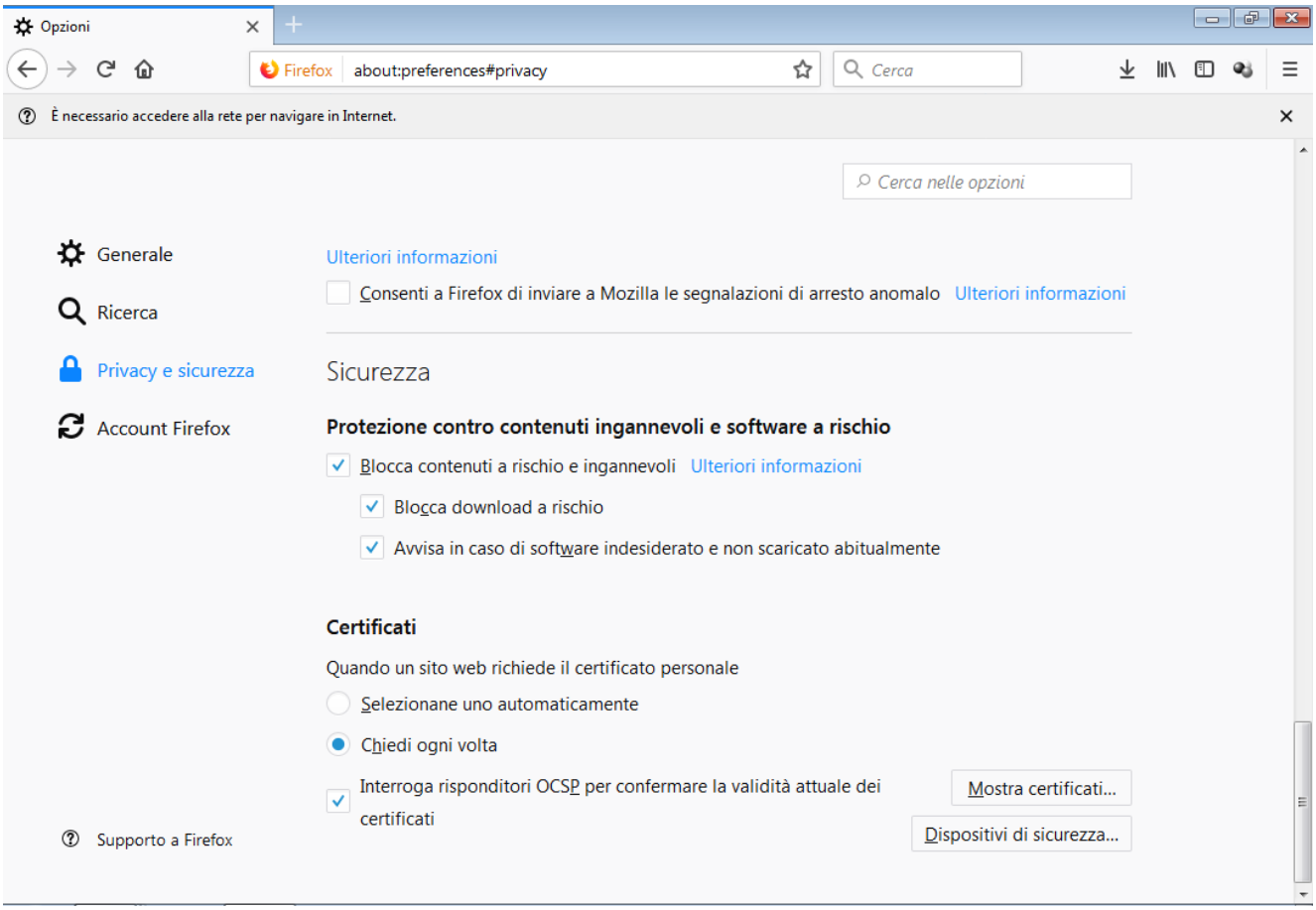
Premere nell'apposito link sulla schermata principale per scaricare il certificato



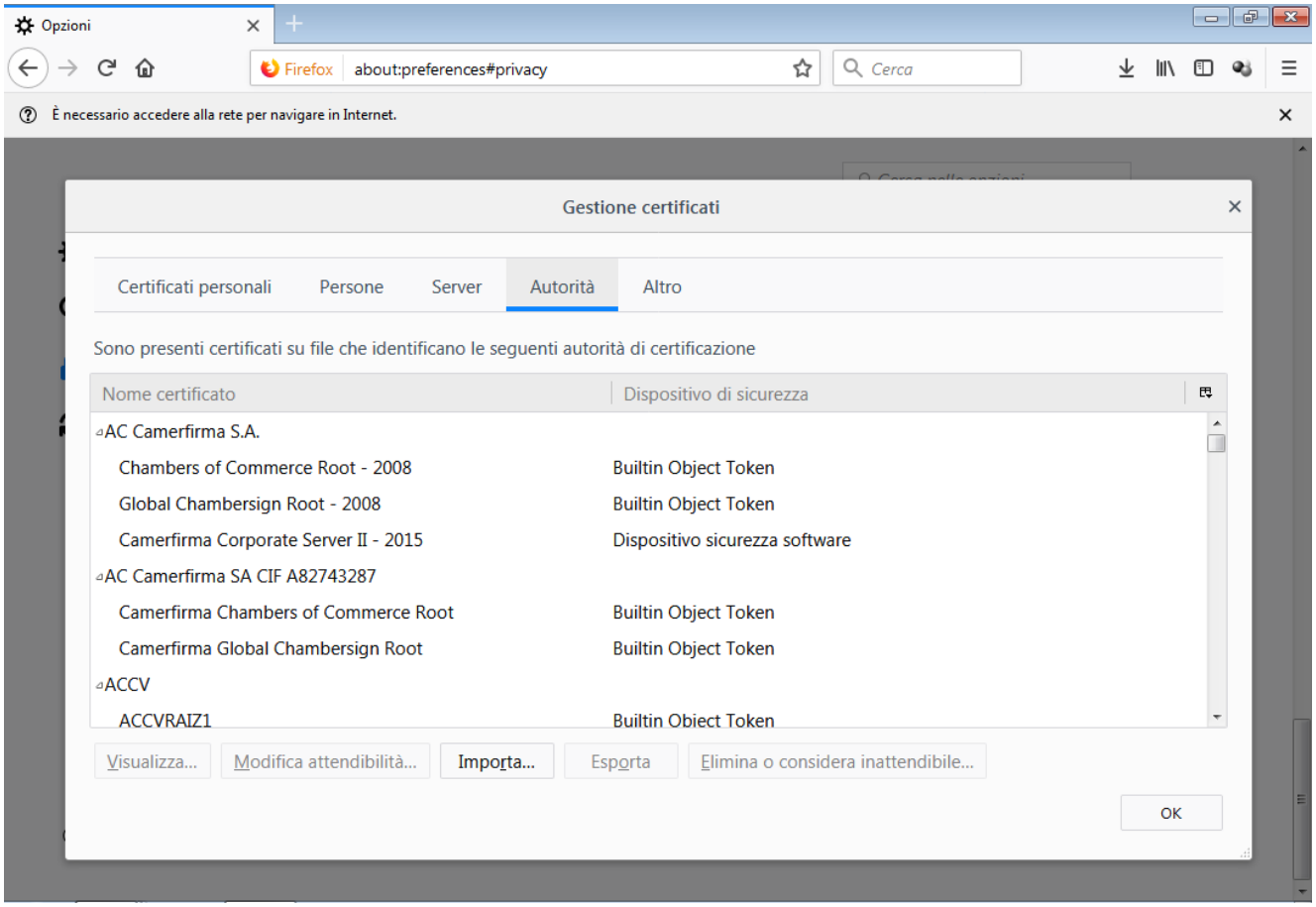
Dopo aver salvato il file del certificato, è necessario eseguire la vera e propria importazione.

Premere sul menu (in alto a destra, icona composta da 3 linee orizzontali), poi premere su Opzioni (icona Ingranaggio), poi nella parte di sinistra premere su Privacy e Sicurezza (icona Lucchetto).

Scorrere adesso tutta la finestra fino a trovare la sezione “Certificati”; premere il pulsante “Mostra Certificati”



Nella finestra che si aprirà, premere sulla sezione “Autorità”



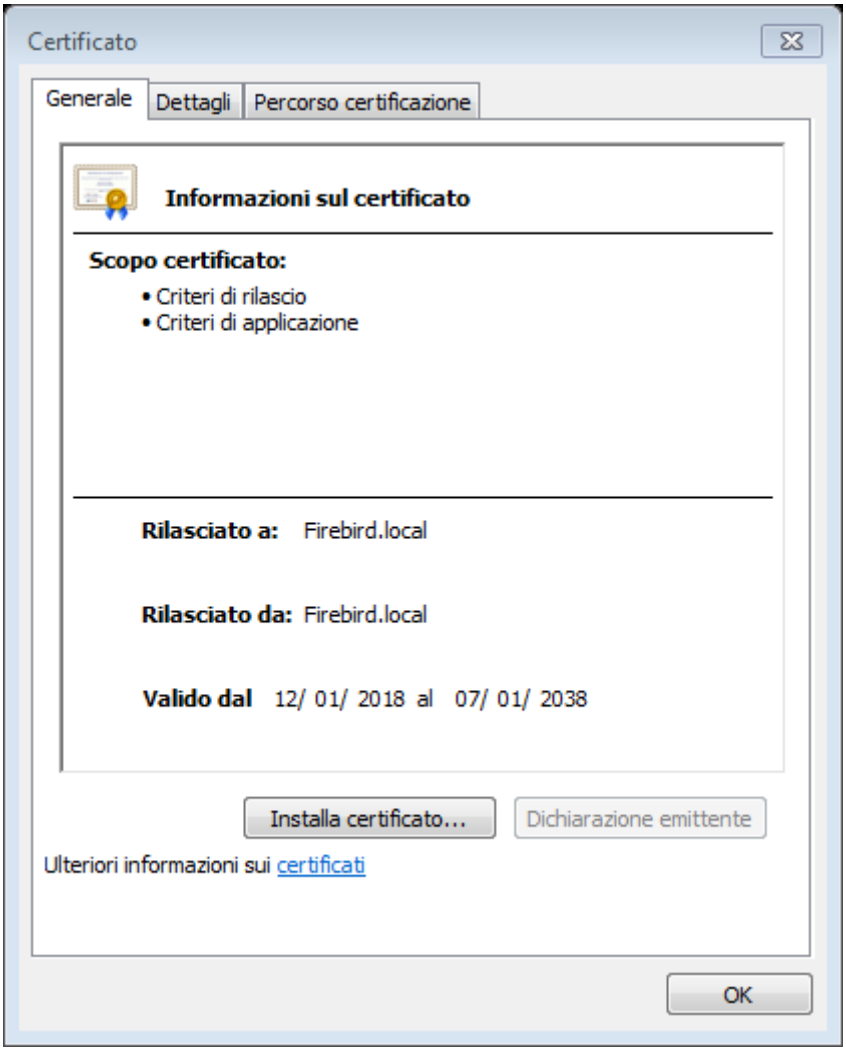
Premere sul pulsante “Importa”, selezionare il file scaricato e dare OK. Il certificato è ora installato.

Installazione su Internet Explorer / Edge

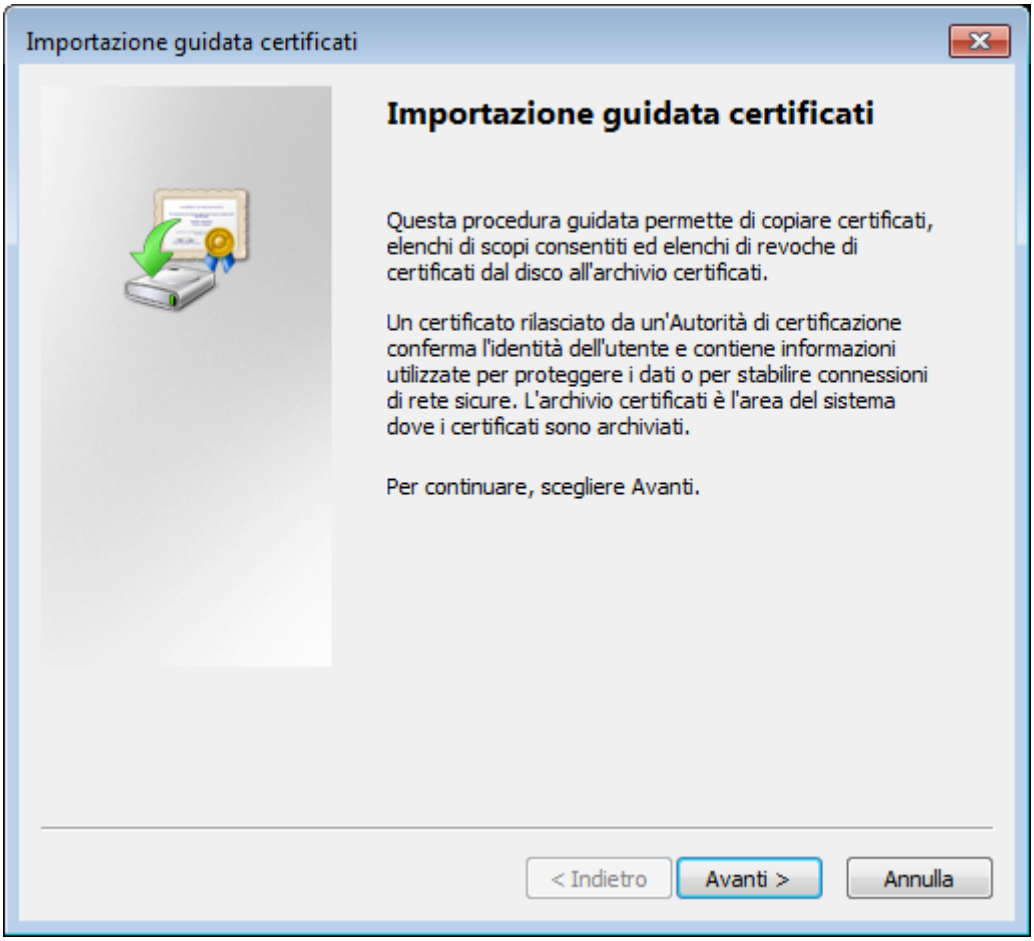
Le seguenti istruzioni riguardano Internet Explorer ma risultano funzionanti anche con Edge.

Eseguire il download del certificato sul PC (vedi sezione precedente)

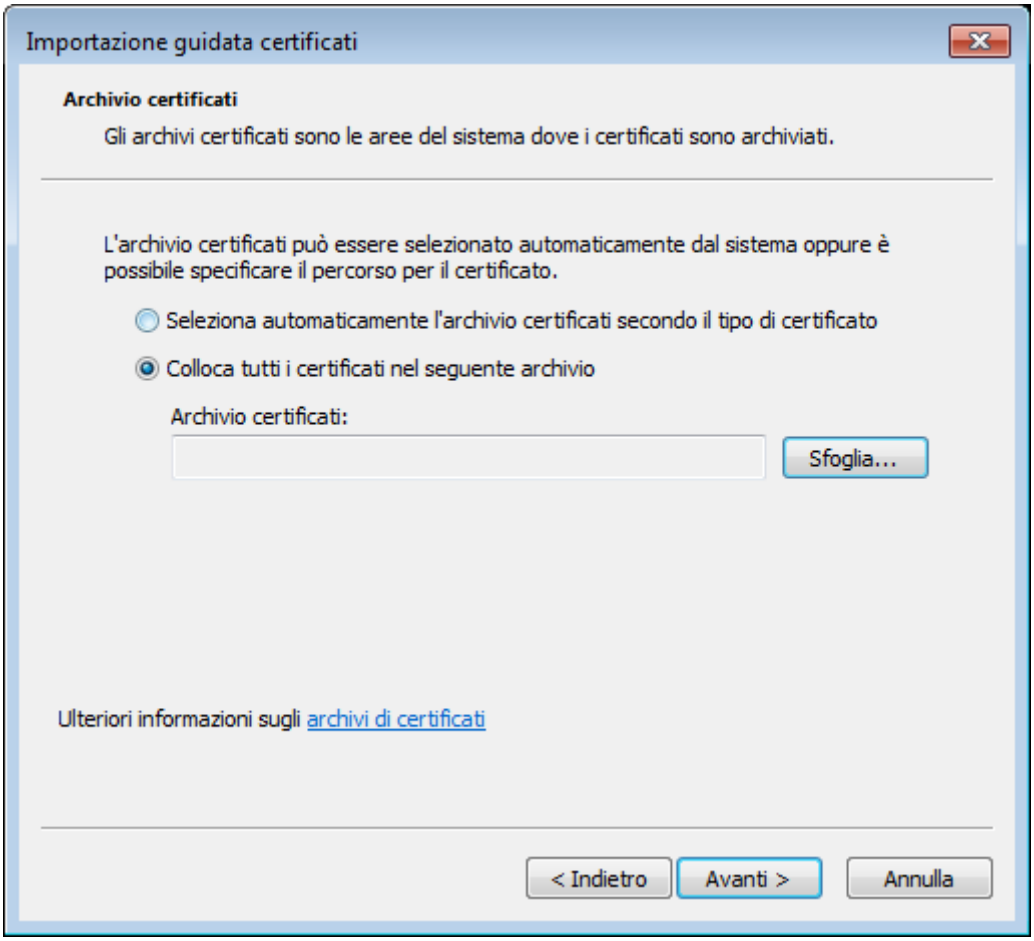
Fare doppio click sul file scaricato, e apparirà la seguente schermata:



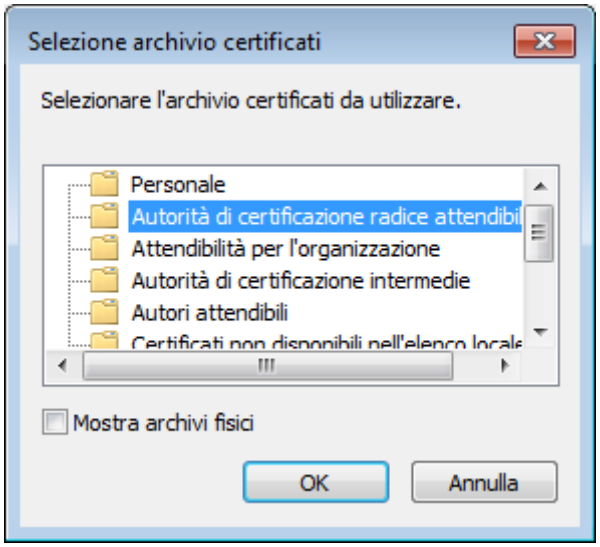
Premere su Installa Certificato



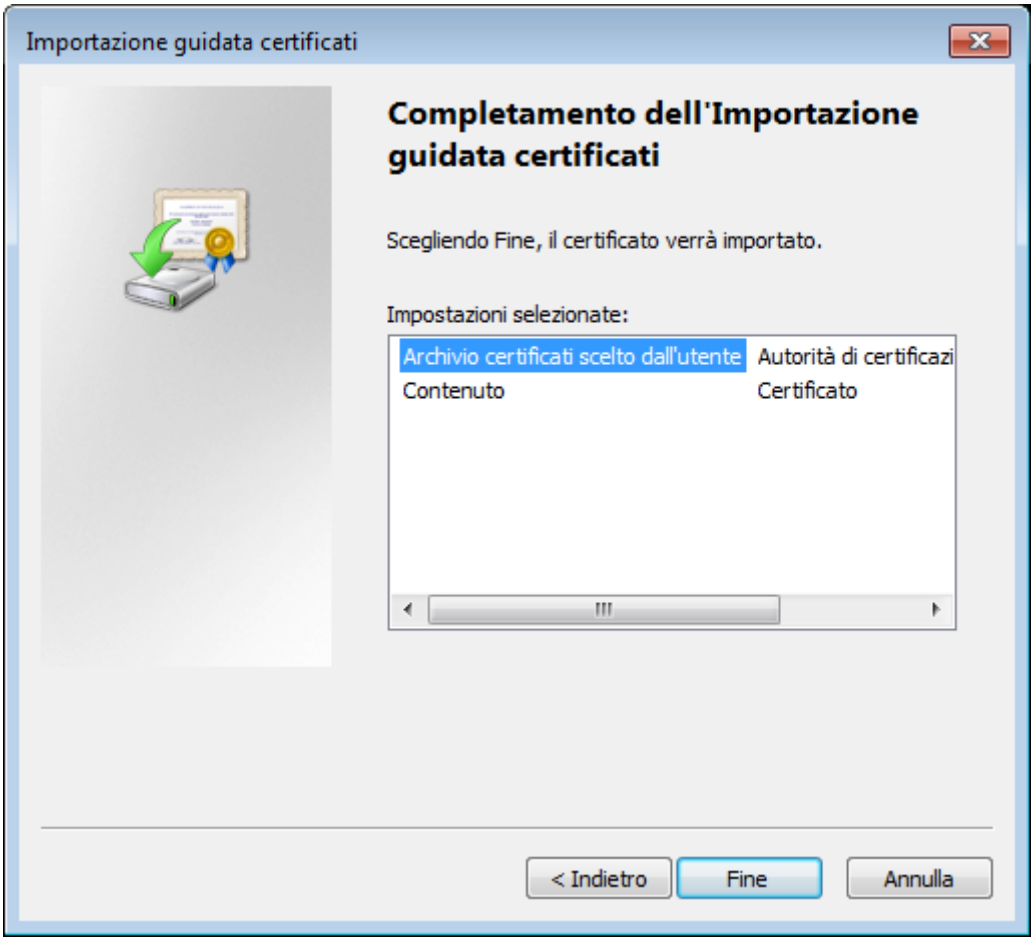
Premere avanti



Selezionare “Colloca tutti i certificati nel seguente archivio”, premere Sfoglia e selezionare “Autorità di certificazione radice attendibili”, come seguente screenshot.



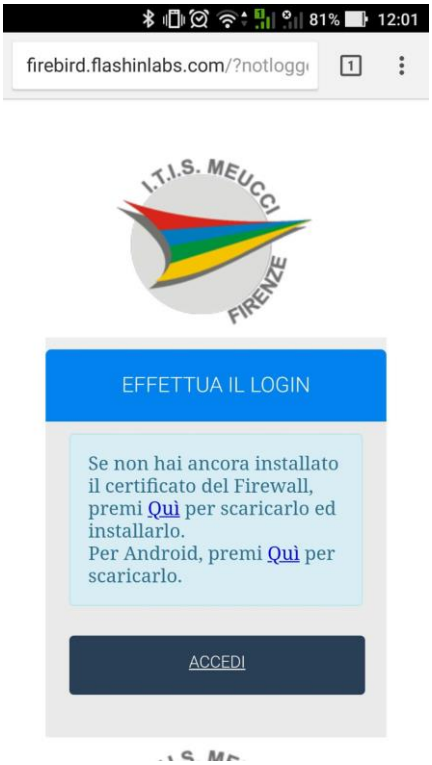
Dopo aver dato conferma a questa schermata premere Avanti, e successivamente Fine.



Il certificato è ora installato.

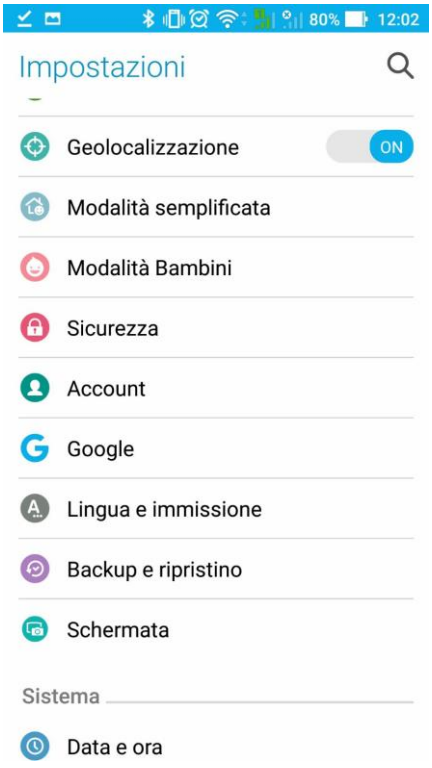
Installazione su Android

Una volta connessi alla rete si presenta la schermata di accesso come segue.

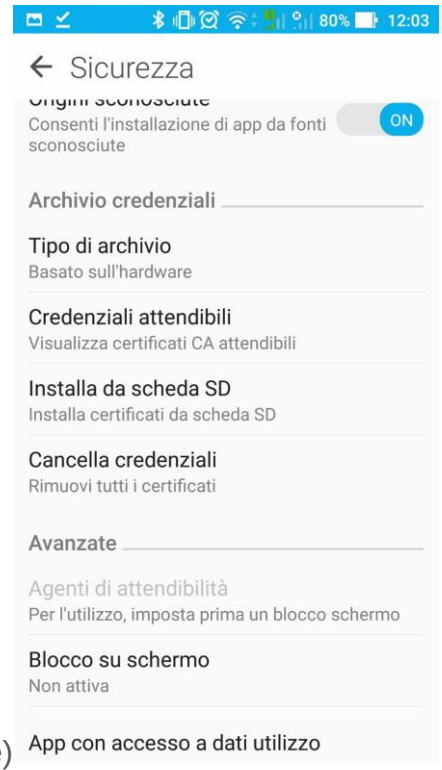


Premere quindi sul link di download per Android, e scaricare il file .pem

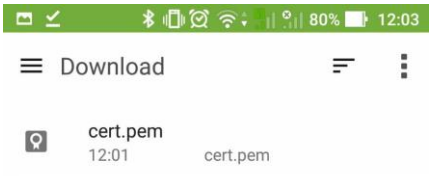
A questo punto andare nel menu Impostazioni del proprio dispositivo Android



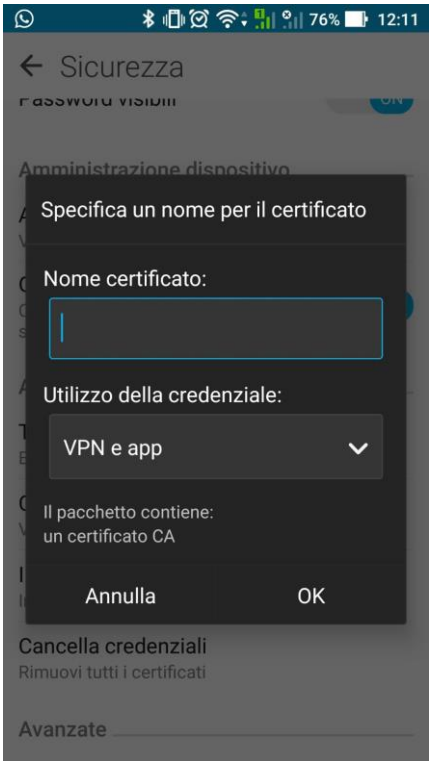
Scorrere fino alla sezione Sicurezza (in alcune versioni può chiamarsi Sicurezza e Posizione)



Premere quindi su Installa da scheda SD

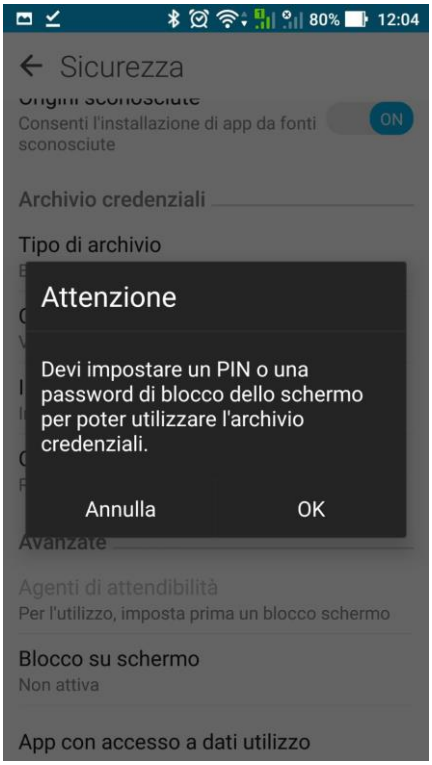


Selezionare quindi il file del certificato per procedere con l’installazione.



Digitare un nome per il certificato, assicurarsi che come utilizzo sia impostato “App” e premere OK. Il certificato risulta quindi installato.

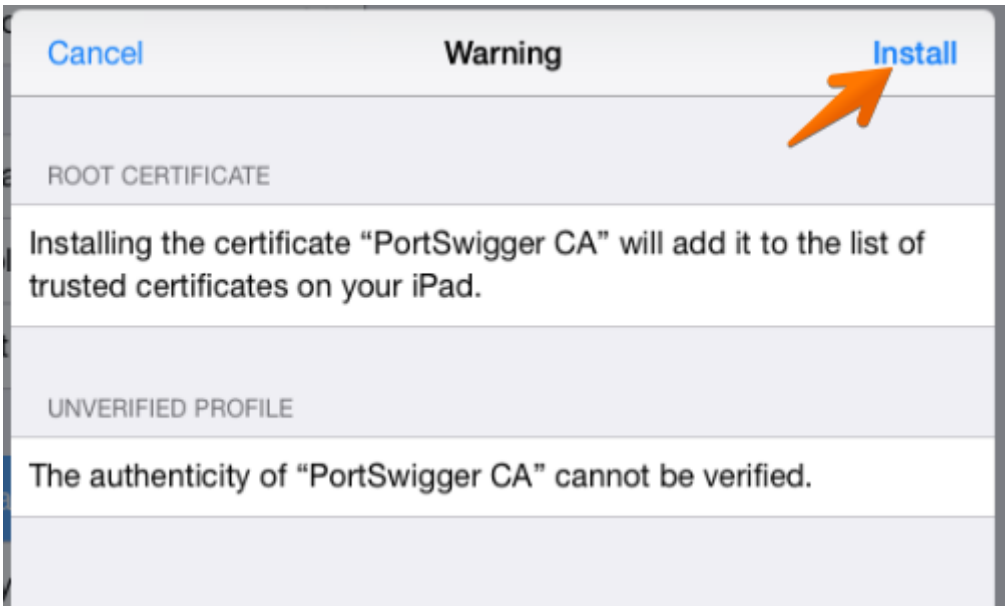
Nota: su alcune versioni di Android, viene richiesto l’attivazione di un blocco schermo per poter procedere all’installazione del certificato; questo limite è imposto dallo stesso sistema operativo.


80% 12:04
Sicurezza
Consenti l'installazione di app da fonti sconosciute
ON
Archivio credenziali
Tipo di archivio
Attenzione
Devi impostare un PIN o una password di blocco dello schermo per poter utilizzare l'archivio credenziali.
Annulla
OK
Avanzate
Agenti di attendibilità
Per l'utilizzo, imposta prima un blocco schermo
Blocco su schermo
Non attiva
App con accesso a dati utilizzo

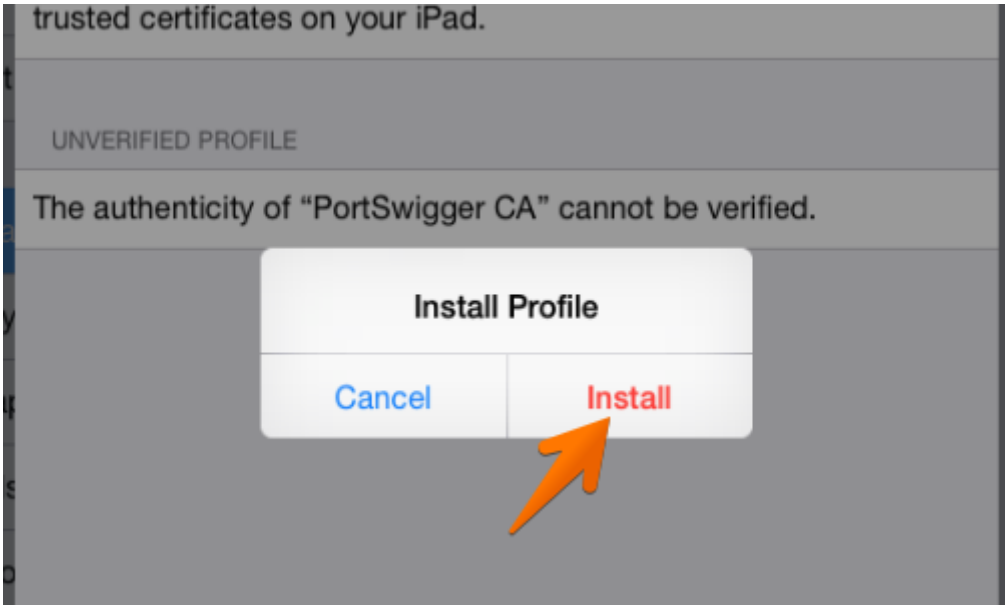
Installazione su IOS

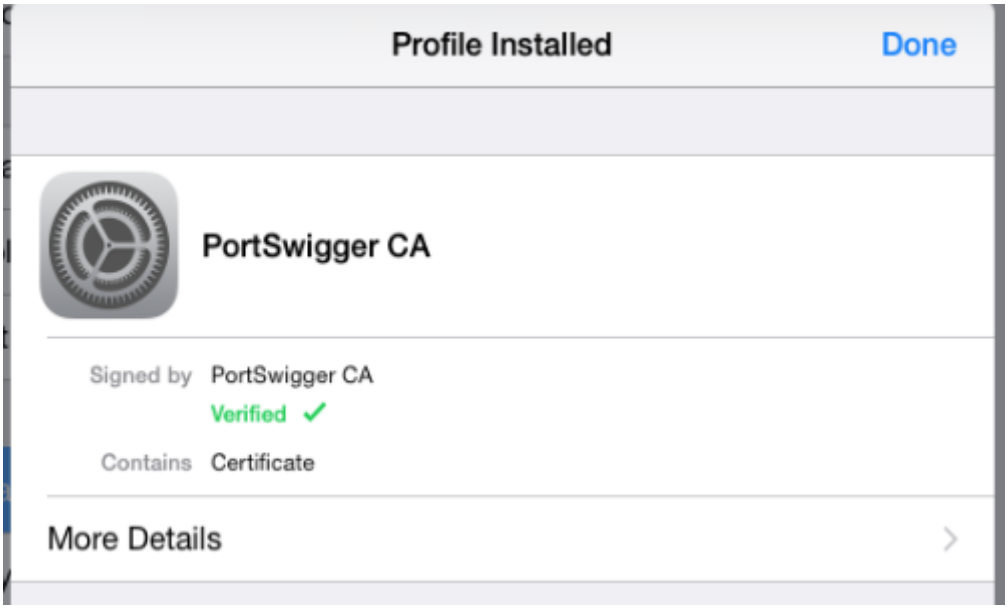
Una volta connessi alla rete si presenta la schermata di accesso, come nei casi precedenti.

Dopo aver eseguito il download del certificato, si presenterà automaticamente la schermata di installazione.



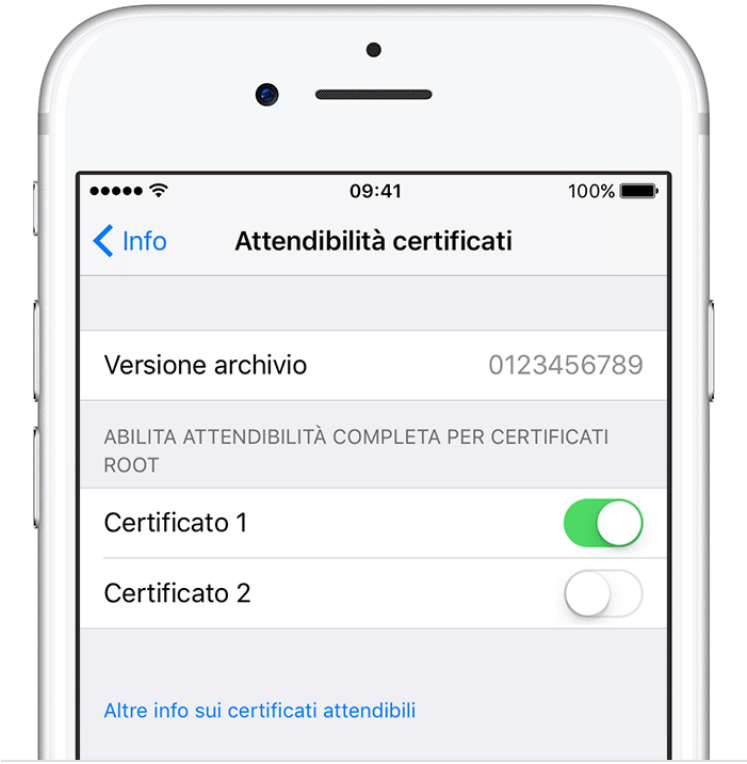
Dopo aver premuto su Installa verrà chiesta una nuova conferma.



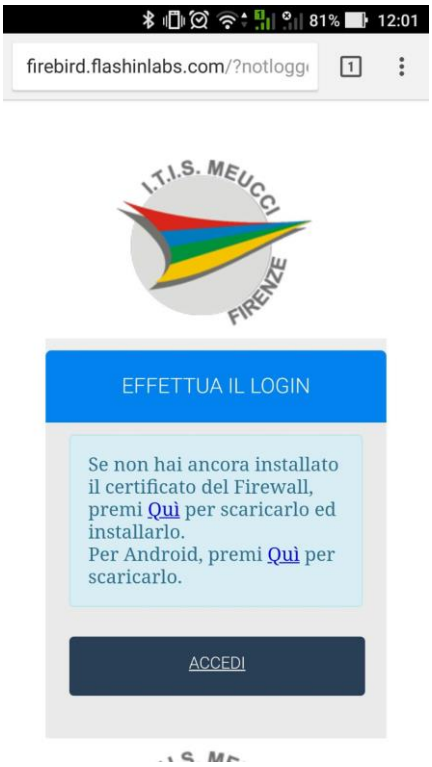


Il certificato risulta quindi installato.

Nota: sulle versioni più recenti di IOS è necessario abilitare l'attendibilità completa del certificato, andando nel menu Impostazioni > Generali > Info > Attendibilità certificati.

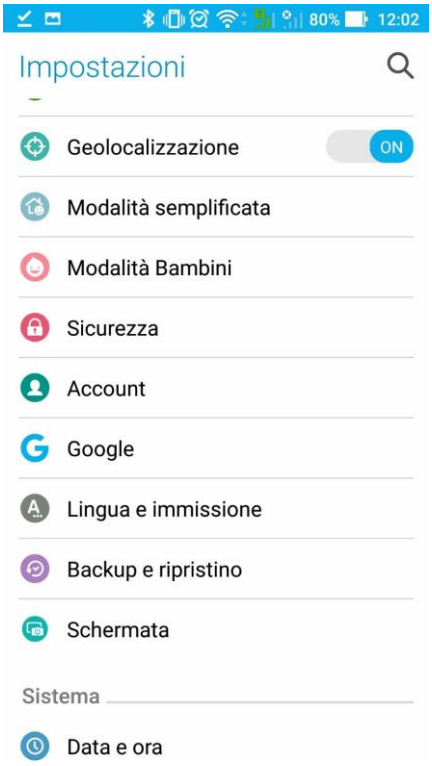


Attivare quindi il certificato installato agendo sulla relativa linguetta.

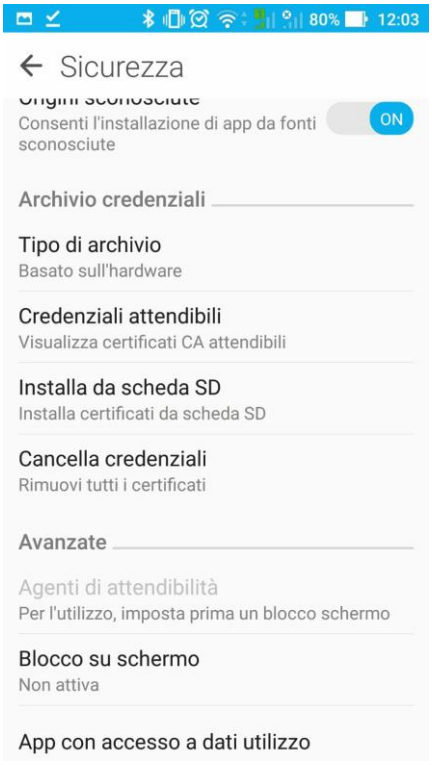


Premere quindi sul link di download per Android, e scaricare il file .pem

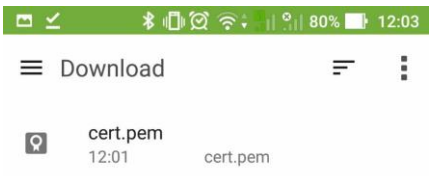
A questo punto andare nel menu Impostazioni del proprio dispositivo Android



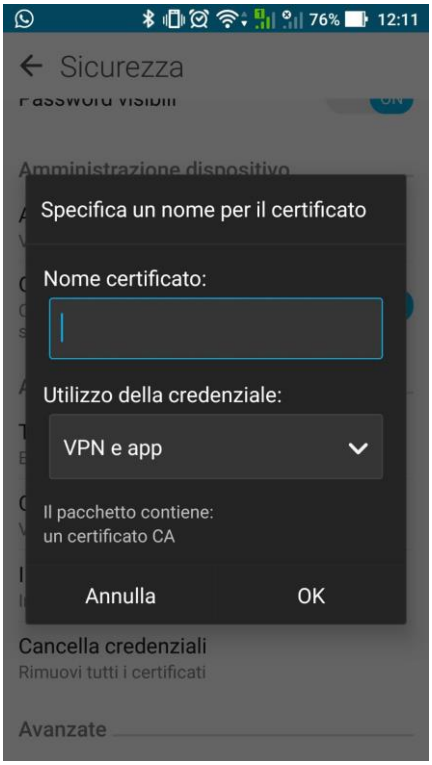
Scorrere fino alla sezione Sicurezza (in alcune versioni può chiamarsi Sicurezza e Posizione)



Premere quindi su Installa da scheda SD



Selezionare quindi il file del certificato per procedere con l'installazione.



Digitare un nome per il certificato, assicurarsi che come utilizzo sia impostato “App” e premere OK. Il certificato risulta quindi installato.

Nota: su alcune versioni di Android, viene richiesto l’attivazione di un blocco schermo per poter procedere all’installazione del certificato; questo limite è imposto dallo stesso sistema operativo.