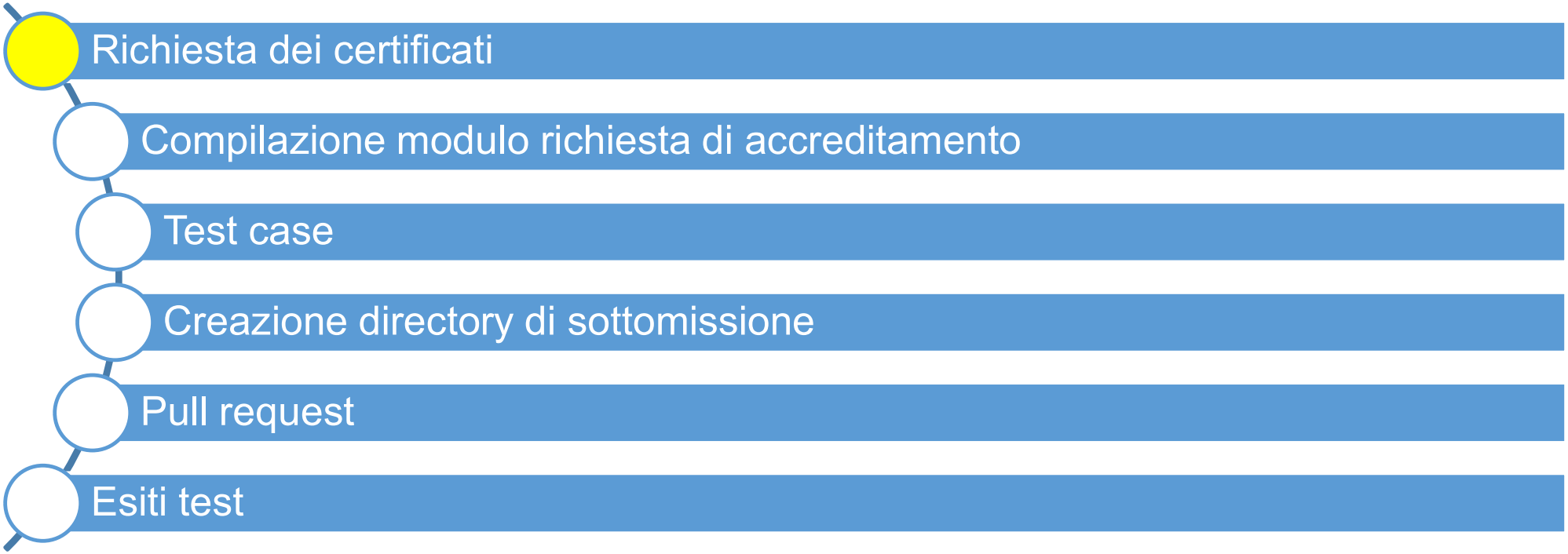
FSE 2.0 – ACCREDITAMENTO AL GATEWAY
Richiesta certificati

Settembre 2023

REGIONE CAMPANIA

Fasi del processo di accreditamento



Richiesta certificati

Il primo passo per il processo di accreditamento consiste nella richiesta dei certificati.

I passi da seguire per poter effettuare tale procedura possono essere consultati al seguente indirizzo https://github.com/ministero-salute/it-fse-support#richiesta-certificati-x509 e sono distinguibili in tre fasi

Ma vediamoli nel dettaglio…

Richiesta certificati 1/3

Generazione CSR

La richiesta di certificati prevede innanzitutto la generazione di Certificate Signing Request (CSR)

La generazione dei CSR è possibile mediante tool come openssl o keytool. Di seguito i dettagli della procedura tramite openssl, già presente in Linux, che può essere scaricato per Windows a partire dal seguente link https://slproweb.com/products/Win32OpenSSL.html

Negli esempi seguenti è stata utilizzata la seguente versione di openssl:

File	Type	Description
Win64 OpenSSL v3.1.2 Light EXE | MSI	5MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v3.1.2 (Recommended for users by the creators of OpenSSL). Only installs on 64-bit versions of Windows and targets Intel x64 chipsets. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.

Richiesta certificati 1/3

Generazione CSR

Ottenuto il tool, dopo l'avvio sarà necessario lanciare due comandi distinti al fine di ottenere il certificato di autenticazione e quello di firma.

Per il certificato di autenticazione sarà necessario lanciare il comando

openssl req -new -newkey rsa:2048 -nodes -keyout chiave_autenticazione_fse_2.0.key -out certificato_autenticazione_fse_2.0.csr

Richiesta certificati 1/3

Generazione CSR

Analogamente, per il certificato di firma bisognerà lanciare il comando

openssl req -new -newkey rsa:2048 -nodes -keyout chiave_firma_fse_2.0.key -out certificato_firma_fse_2.0.csr

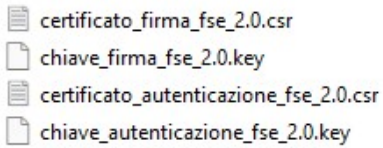
```
C:\Users\F.Romano\Documenti>"C:\Program Files\OpenSSL-Win64\bin\openssl" req -new -newkey rsa:2048 -nodes -keyout chiave_firma_fse_2.0.key -out certificato_firma_fse_2.0.csr
....+......+.......+.........+...++++++++++++++++++++++++++++++++++++++++++++.+...+.....+.++++++++++++++++++++++++++++++++++++++++++++.+.........................+.......+.....+...+....+........+...+....+...+.....
.......+......+...+.......+...+......+...+...+..+.+..............+.+.....+....+..+.+........+....+........+.......+...+.....+........+....+..+.........+......+.........+...+..+..
...................+............+..............++++++
............+.+......+..+...++++++++++++++++++++++++++++++++++++++++.+.....................+.++++++++++++++++++++++++++++++++++++++++....+..........+.........+.+.............+.......+...........+...+......+.
..+.+..+............+..+...........+...+...+.+...+.....+.+...........+...........+........+...+.....+.....+.......+.....+..........+.....+...+.+.....+..+.............+......+.+.............+....
....+...+...+.......+........+..........+..........+......+...+....+...+...+.....................+...+.....+....+...+....+....+.....+..........+...+..+....+.........+.+......+.....+.+.........+
..+.+..............+..+...+...+......+...+...+...+.......+.....+...+.......+...+..+............+.........+...+..+...+.....................+......+.......+..+........+....+..+...+.....+......+.+..+......
.........+.+......+...+......+......+.....+..........+......+.....+...+.......+..............+..............+...+......+...+..+...+...+...+.....+...+...+.+...+...........+.+.............+...........+..
.+.+......+...+............+............+.................+........+....+.....+..............+.+..+....+........+...+....+.........+...........+.............++++++
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IT
State or Province Name (full name) [Some-State]:NAPOLI
Locality Name (eg, city) []:NAPOLI
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Almaviva spa
Organizational Unit Name (eg, section) []:Market Domains Practice & Governance
Common Name (e.g. server FQDN or YOUR name) []:Fortuna Romano
Email Address []:f.romano@almaviva.it

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Richiesta certificati 1/3

Generazione CSR

A conclusione dell'elaborazione, verranno generati i due certificati e le corrispettive key.



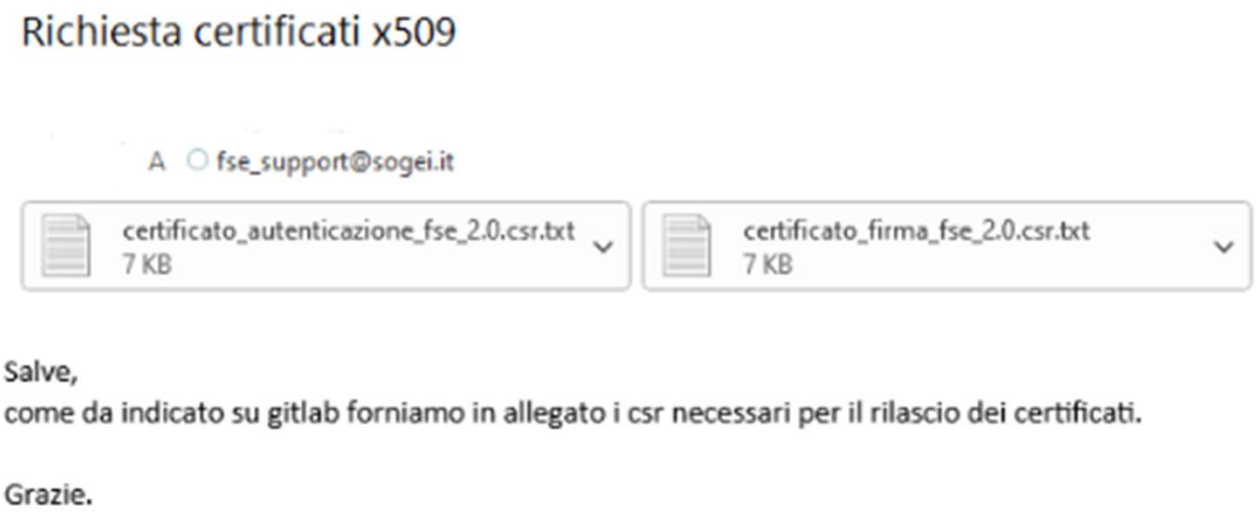
Mentre i due file .csr saranno oggetto di invio per l'avanzamento della procedura, le due chiavi dovranno essere salvate in locale e non condivise con terzi.

Fondamentale è la conservazione delle chiavi (file .key) in quanto saranno necessarie, insieme ai certificati che verranno consegnati, per l'accesso ai servizi del Gateway

Richiesta certificati 2/3

Invio CSR

I file CSR ottenuti dovranno essere inviati tramite mail all'indirizzo «fse_support@sogei.it».


Richiesta certificati x509

A fse_support@sogei.it

certificato_autenticazione_fse_2.0.csr.txt
7 KB

certificato_firma_fse_2.0.csr.txt
7 KB

Salve,
come da indicato su gitlab forniamo in allegato i csr necessari per il rilascio dei certificati.

Grazie.

Risulta utile, prima dell'invio, aggiungere l'estensione .txt, per evitare eventuali blocchi degli allegati in fase di invio della mail.

Richiesta certificati 3/3

Ottenimento certificati

Come risultato dell'invio dei due CSR, Sogei, nell'arco di alcuni giorni, risponderà trasmettendo i due certificati necessari per il proseguimento della procedura di accreditamento.


R: Richiesta certificati x509

F

fse_support <fse_support@sogei.it>

A

Flag for follow up.

ALMAVIVAXX_CERT.zip
3 KB

Salve,

in allegato i certificati richiesti.

Un saluto,
Il team FSE2.0

I due file contenuti nel .zip allegato saranno da utilizzarsi, insieme alle chiavi ottenute mediante openssl, per l'accesso ai servizi del Gateway.

Richiesta certificati

In particolare, per poter avviare tutta la procedura per l'invocazione del Gateway, a partire dai due file .pem inviati da Sogei, sarà necessario generare i due corrispondenti file .p12 mediante il tool opnelssl.
Per ottenere i file .p12 di autenticazione e di firma, una volta entrati nella directory contenente i .pem e i .key, bisognerà lanciare i seguenti comandi

openssl pkcs12 -export -out chiave_autenticazione_fse_2.0_.p12 **-in** A1#111ALMAVIVAXX.pem **-inkey** chiave_autenticazione_fse_2.0.key **-name** autenticazione

openssl pkcs12 -export -out chiave_firma_fse_2.0.p12 **-in S1#111ALMAVIVAXX.pem -inkey** chiave_firma_fse_2.0.key **-name** firma

Il valore dell'attributo «name» del file .p12 può essere imposto e letto anche tramite il tool «KeyStore Explorer» settando o visualizzando l'attributo EntryName.
Il tool può essere scaricato qui : https://keystore-explorer.org/downloads.html

Richiesta certificati

```
C:\Users\                                   "C:\Program Files\OpenSSL-Win64\bin\openssl" pkcs12 -export -out c
hiave_autenticazione_fse_2.0_.p12 -in A1#111ALMAVIVAXX.pem -inkey chiave_autenticazione_fse_2.0.key -name autenticazione

Enter Export Password:
Verifying - Enter Export Password:

C:\Users\                                   >openssl pkcs12 -export -out chiave_firma_fse_2.0.p12 -in S1#111ALM
AVIVAXX.pem -inkey chiave_firma_fse_2.0.key -name firma
Enter Export Password:
Verifying - Enter Export Password:
```

Grazie a tale procedimento verranno generati i due file .p12 che utilizzeremo durante la procedura per l'invocazione del Gateway.

Richiesta certificati

I certificati emessi da Sogei hanno una scadenza che è possibile verificare utilizzando il comando openssl:

openssl x509 -enddate -noout -in "percorso del certificato"

Si ottiene in risposta la data di scadenza in questo formato:

notAfter=MM dd HH:mm:ss yyyy GMT

Se il certificato è scaduto è necessario effettuare nuovamente la richiesta.

Grazie

REGIONE CAMPANIA