Quaderno di progetto

# Generazione delle credenziali di accesso alla VPN

Autori: C. Gaibisso, B. Martino
Ultima revisione: 04 marz0 2019
Versione: 1.1

## Sommario

# 1 Contenuto

Questo documento illustra nel dettaglio il processo di generazione delle credenziali di accesso alla *Virtual Private Network* di Istituto, *VPN* in quanto segue. Tale processo si concretizza in un file compresso e cifrato contenente i tre file di configurazione del client di *openVPN*, denominato *client VPN* in quanto segue, da utilizzarsi in ambiente *Windows*, *Ubuntu* e *MacOS*.

# 2 Caratteristiche della soluzione software

È opportuno ricordare che la *VPN*, che garantisce un accesso sicuro, anche da reti diverse dalla 150.146.5.x (reti interene all'edificio di Via dei Taurini), ai servizi telematici di Istituto, ricorre alle funzionalità offerte da *Easy-RSA (vers. 3.0.6)* per l'implementazione di una soluzione open source di *PKI (Public Key Infrastructure)*, in grado, tra l'altro, di:

- dotare i server che erogano i servizi, e gli utenti che li utilizzano, delle credenziali digitali (chiave privata e certificato digitale) necessarie al reciproco riconoscimento e a cifrare le comunicazioni;
- svolgere le funzionalità tipiche di una *Certification Authorithy (CA)*. Tale soluzione è riferita come *Server CA*, in quanto segue.

Il *Server CA*, al quale per motivi di praticità e di sicurezza è delegato tutto il processo di generazione delle credenziali, è ospitato da una VM *Oracle VM Virtual Box (vers. 6.0)*, raggiungibile all'indirizzo è 150.146.5.224.

# 3 Generazione delle credenziali elettroniche

Sul *Server CA (system)*

a) Posizionati nella directory EasyRSA-v3.0.6

```
$ cd ~/EasyRSA-v3.0.6/
```

b) Genera la richiesta di certificato (*nomeCognome.req*) e la chiave privata del *Client VPN* (*nomeCognome.key*)

```
$ ./easyrsa gen-req nomeCognome nopass
```

Quando richiesto

```
Common Name (eg: your user, host, or server name) [nomeCognome]:
```

conferma la scelta di default con un *return*

*Output*

```
. . .

Keypair and certificate request completed. Your files are:
req: /home/system/EasyRSA-v3.0.6/pki/reqs/nomeCognome.req
key: /home/system/EasyRSA-v3.0.6/pki/private/nomeCognome.key
```

c) Copia la chiave privata del *Client VPN* nella directory */client-configs/keys/*

```
$ cp pki/private/nomeCognome.key ~/client-configs/keys/
```

d) Genera, a partire dalla richiesta, il certificato pubblico del *Client VPN* (*nomeCognome.crt*)

```
$ ./easyrsa sign-req client nomeCognome
```

*Output*

```
Note: using Easy-RSA configuration from: ./vars

Using SSL: openssl OpenSSL 1.1.0g  2 Nov 2017

You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a client certificate for 1080 days:

subject=
    commonName                = nomeCognome

Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes
Using configuration from /home/system/EasyRSA-v3.0.6/pki/safessl-easyrsa.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'nomeCognome'
Certificate is to be certified until Jan 26 16:14:44 2022 GMT (1080 days)

Write out database with 1 new entries

Data Base Updated

Certificate created at: /home/system/EasyRSA-v3.0.6/pki/issued/nomeCognome.crt
```

e) Copia il certificato pubblico del *Client VPN* nella directory */client-configs/keys/*

```
$ cp ~/EasyRSA-v3.0.6/pki/issued/nomeCognome.crt ~/client-configs/keys/
```

# 4 Generazione dei file di configurazione

Per il richiedente *Nome Cognome*

Sul *Server CA (system)*

a) Posizionati nella cartella ~/client-configs

```
$ cd ~/client-configs
```

b) Genera i file di configurazione di openVPN per i sistemi Windows, Ubuntu e MacOS

```
$ ./makeConfigs.sh nomeCognome
```

Al termine, troverai i tre file di configurazione *nomeCognomeWin.ovpn*, *nomeCognomeUbuntu*.ovpn e *nomeCognomeMacOS.ovpn* nella directory *~/client-configs/files*

c) Posizionati nella cartella ~/client-configs

```
$ cd ~/client-configs
```

d) Comprimi e cifra i tre file di configurazione nel file *nomeCognome.zip*

```
$ zip --password <Password> nomeCognome.zip nomeCognome*.ovpn
```

# 5 Generazione automatica dei file di configurazione

I procedimenti descritti nel dettagio nelle sezioni 3 e 4 sono codificati nello script:

*/home/system/client-configs/createVpnUser.sh.*

che prevede due parametri: nome e cognome del *Client VPN*, nel formato *nomeCognome*, e la password necessaria a cifrare/decifrare il file compresso *nomeCognome.zip*

# 6 Revision history

| Data | Versione | Descrizione | Autori |
|---|---|---|---|
| 28 febbraio 2019 | 1.0 | • Rilascio | Carlo Gaibisso<br>Bruno Martino |
| 04 marzo 2019 | 1.1 | • Approtate minime modifiche | Carlo Gaibisso<br>Bruno Martino |

# 7 Task

| Task | Data Inserimento | Data Inizio | Data Termine | Note |
|---|---|---|---|---|
| | dd/gg/aaaa | dd/gg/aaaa | dd/gg/aaaa | |
| | dd/gg/aaaa | dd/gg/aaaa | dd/gg/aaaa | |