Readme file for system users

Fredrik Krantz
fkra@kth.se
940322-9355

Ruizhi Yang
ruizhi@kth.se
980722-1610

Xin Liu
xinl2@kth.se
951019-9384

March 13, 2020

1 Introduction

This is a readme file on how to use the system we have implemented.

2 Authentication using OpenSSL

2.1 Steps of Mutual Authentication

1. A protected service present on a server is requested by client
2. Server sends its certificate to the client
3. The client verifies the server's certificate
4. Client then sends its certificate to the server
5. The server verifies the client's certificate
6. Once the verification is successful, client is able to execute the protected service

2.2 Implementation Details of Client part

1. Install OpenSSL
   You can find the repository in this website: https://github.com/openssl/openssl
2. Generate private key using OpenSSL

   ```
   openssl genrsa -out client-key.pem 2048
   ```

3. Submit a CSR to CA using OpenSSL

   ```
   openssl req -new -sha256 -key client-key.pem -out clientA-csr.pem
   ```

4. Receive the signed certificate from CA

3 OpenVPN setup manual

3.1 Linux

Step 1: Install OpenVPN using command: apt-get install OpenVPN,
Step 2: Download the configure file provided by ACME and unzip it,
Step 3: Start OpenVPN on this configure file with the follwing command: openvpn client.ovpn .

3.2 Windows

Step 1: Download OpenVPN https://openvpn.net/community-downloads/, then install it,
Step 2: Download the configure file provided by ACME and unzip it,
Step 3: Open the configure file *client.ovpn* with Openvpn
Step 4: Start connection

3.3 Mobile devices

Step 1: Download OpenVPN from Playstore(Android) or Appstore(IOS),
Step 2: Download the configure file provided by ACME and unzip it,
Step 3: Open the configure file *client.ovpn* with Openvpn
Step 4: Start connection

4 Wireless connection

In order to connect to the wireless network you first need to have a authorized account setup on the RADIUS server. Make sure to contact your system administrator in order to get one. Then you just connect to the Acme-London-wifi with your credentials.

5 Nextcloud usage

After connecting to the nextcloud server ip you login with your provided credentials. Make sure to install google authenticator on your mobile device in order to sync it to your nextcloud account. In order to access the nextcloud fileserver from the london office you need to setup the VPN-client first and you need to be connected to the London local network. For manual on the nextcloud service see:
https://docs.nextcloud.com/server/18/user_manual/