MUM INDONESIA ON DECEMBER 05 - 06, 2014

Open SSL Certificate (HTTPS) for Mikrotik Hotspot Login



About me



Aldi Nor Fahruin

Using Mikrotik since 2012

Freelance at PT Proxis Indonesia Solution

CV. Cipta Satmedia

Universitas Teknologi Yogyakarta

Certification:

MTCNA (Mikrotik Certified Network Associate) 2014

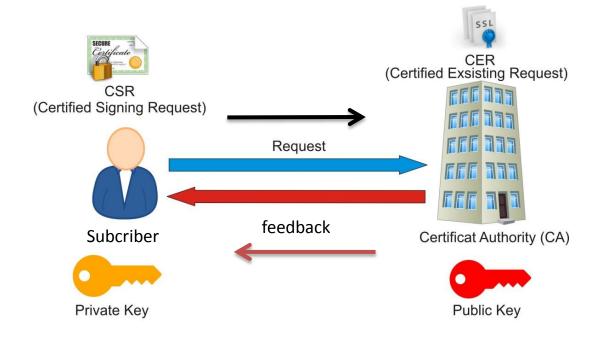


Digital Certificate Infrastructur and Concept





Digital Certified Concept



Digital certificate -> identity card

Certificate Authority -> sovereign issued a certificate/ Government

Subcriber - > User Request

CSR (Certified signing request) -> Proposal



Self-Signed Certificate



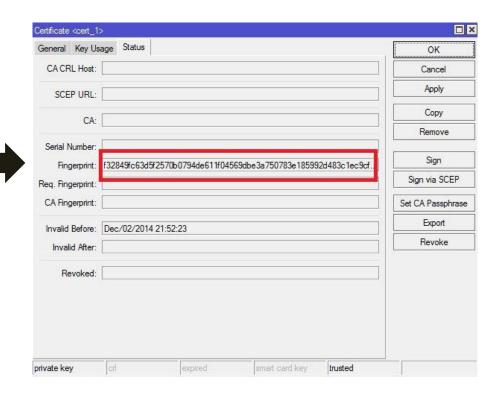


----BEGIN CERTIFICATE----

MIICWzCCAcQCCQcousge1PITuDANBgkqhkiG9w0BAQUFADBxMQswCQYDVQQGEwJJ
RDEMMAoGA1UECBMDRE1ZMRMwEQYDVQQHEwpZb2d5YWthcnRhMQwwCgYDVQQKEwNN
VU0xDTALBgNVBAMTBEFMREkxIjAgBgkqhkiG9w0BCQEWE2FrdW5fYWxkaUB5YWhv
by5jb20wIBcNMTQxMjAyMTQ1MjIzWhgFMTkwNjAzMTQwODI0MDdaMHExCzAJBgNV
BAYTAk1EMQwwCgYDVQQIEwNESVkxEzARBgNVBAcTC1lvZ3lha2FydGExDDAKBgNV
BAoTA01VTTENMAsGA1UEAxMEQUxESTEiMCAGCSqGSIb3DQEJARYTYWt1b19hbGRp
QHlhaG9vLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAvjIcPx/gzeYQ
QewJIpxetRvi0sBkEEYV1FT6QU2dwKTqqmW/YQJrZvSfveuNP5zR02By18tKLF4b
YgxBkyRkBUkjFIa0YizsJ6Xpnbnjsas7SbOmVFED2yUC57nVpHEwf6wiAZohZhp1
mYMelpNnrtCFY80KLUPaqba41/m+YR8CAwEAATANBgkqhkiG9w0BAQUFAAOBgQBu
8ARumDM/9X46WkptZtkbEJ+UDXLMwJr0M4vvSA52ugIUQFObr00YxXbUxumfpcLD
oxp49S/qGgiiirYAIg+L0QY0ulDmZ6UxI0Yi46gZ/auUDDaiQimqB6ogYQlcwZUZ
rAHiMNxQyWJj2SIDV9Jrivs1XLl0tMzfDkoy4ptJ1Q==

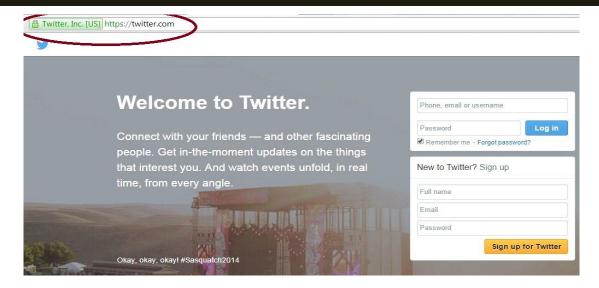
----END CERTIFICATE----







Difference Self-Signed Certificate and Signed by Certificate Authority





Signed by Certificate Authority



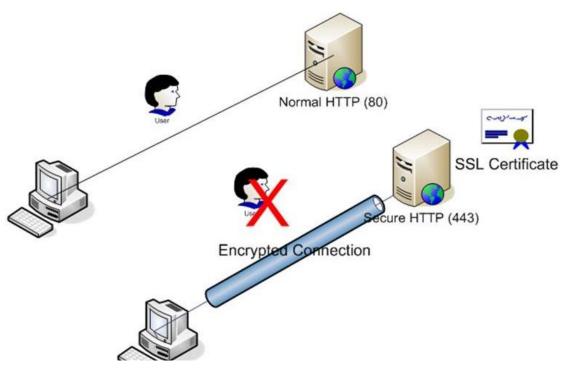


Self-Signed Certified



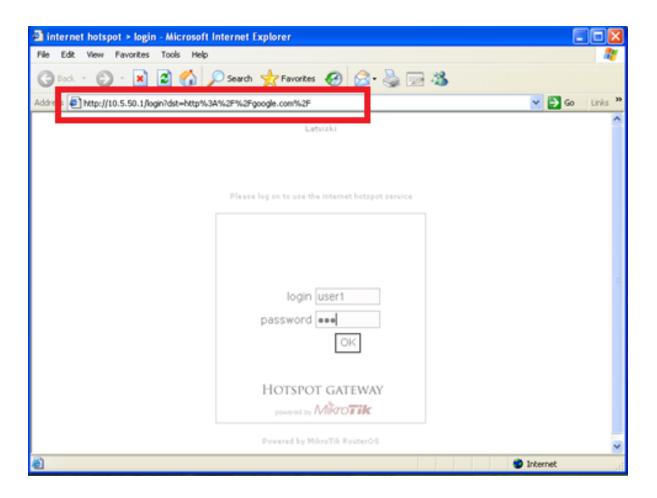
HTTP vs HTTPS

HTTP vs HTTPS



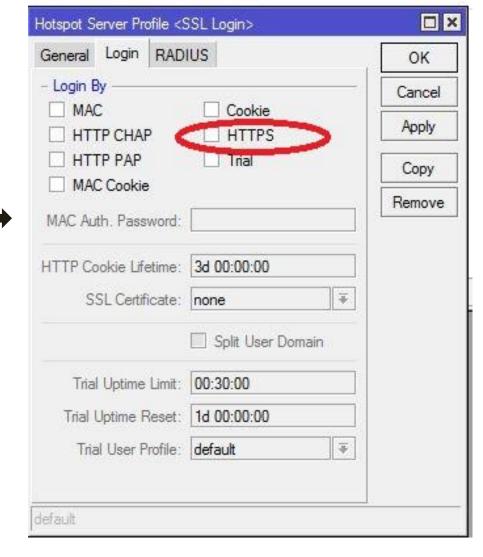


By default Mikrtotik hotspot login use protocol http





Mikrotik Hotspot Feature





Lab Demo



1. Generate new private key

openssl genrsa -des3 -out hotspot.key 1024

```
Generating RSA private key, 1024 bit long modulus
......+++++
e is 65537 (0×10001)
Enter pass phrase for hotspot.key: <password>
Verifying - Enter pass phrase for hotspot.key: <ulangle password>
```



2. Generate certificate signing request (CSR)

openssl req -new -key hotspot.key -out hotspot.csr

Enter pass phrase for hotspot.key: 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) [GB]:ID State or Province Name (full name) [Berkshire]:DIY Locality Name (eg, city) [Newbury]: Yogyakarta Organization Name (eg, company) [My Company Ltd]: CIPTASATMEDIA Organizational Unit Name (eg, section) []:. Common Name (eg, your name or your server's hostname) []: hotspot.Ciptasatmedia.com Email Address []; hotspot@gmail.com Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []:<password> An optional company name []:Badan Sistem Informasi

Will be made file hotspot.csr based hotspot.key



3. Generate certificate signing request (CSR) based on exsisting certified openssl x509 -req -days 10000 -in hotspot.csr -signkey hotspot.key -out hotspot.crt

Signature ok subject=/C=ID/ST=DIY/L=Yogyakarta/O=UII/CN= hotspot.Ciptasatmedia.com/emailAddress=hotspot@gmail.com
Getting Private key
Enter pass phrase for hotspot.key: <password>

Will make file certificate ssl hotspot.crt based on points one and two

4. Upload file hotspot.key and hotspot.crt to Mikrotik router Mikrotik by using FTP



4. installation certified at Mikrotik Router

5. see the results of installasi

/Certficate Print

/certificate import file-name=hotspot.crt

passphrase: <password> certificates-imported: 1 private-keys-imported: 0

files-imported: 1

decryption-failures: 0

keys-with-no-certificate: 0

/certificate import file-name=hotspot.key

passphrase: <password> certificates-imported: 0 private-keys-imported: 1

files-imported: 1

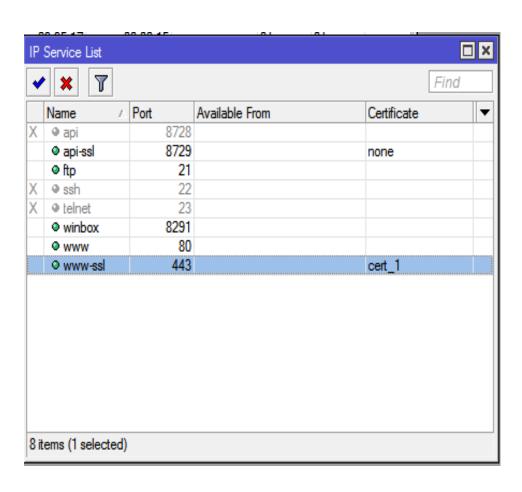
decryption-failures: 0

keys-with-no-certificate: 0

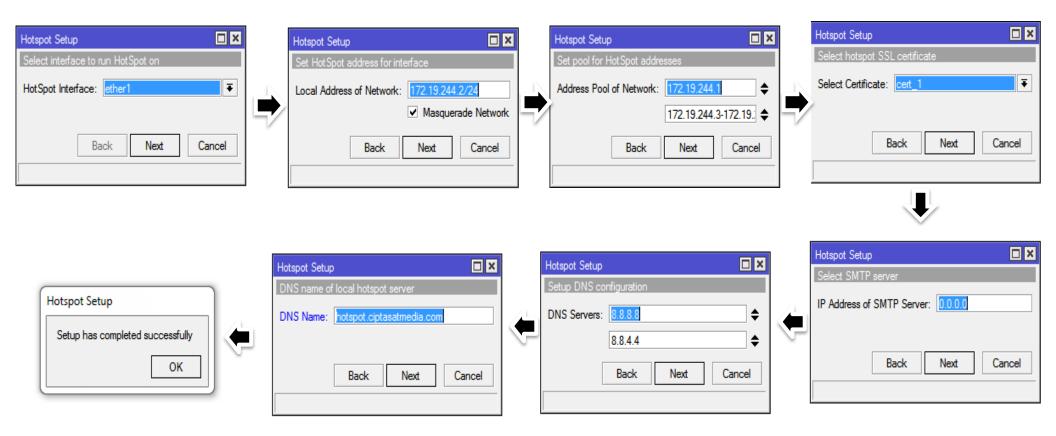


6. Plug connection www-ssl with certificate cert1 who finished in import

/ip service set www-ssl certificate=cert1

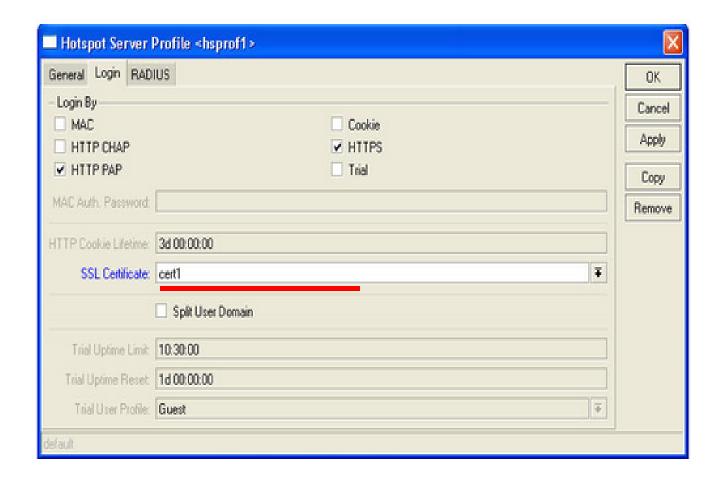


7. Create Hostpot Mikrotik



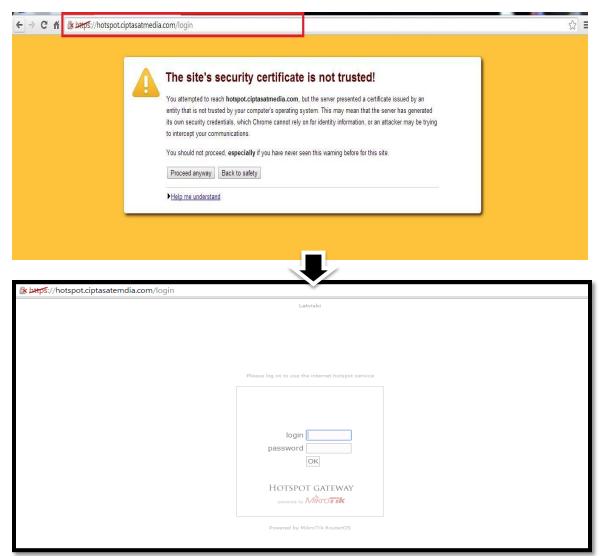


7. Make sure server profile hotspot can be connected with https and certificate cert1





8. then try to access the hotspot









akun_aldi@yahoo.com



+62 8564 3904 438



Aldi N Fahrudin