OpenSSL Usage

Stefan Hornburg (Racke)

Contents

Useful site with SSL commands, CSR and certificate decoder:
`https://redkestrel.co.uk/articles/openssl-commands/`

Display certificate request

```
$ openssl req -noout -text -in /etc/apache2/ssl/server2016.csr
```

Display to whom it was issued from PEM file

```
$ openssl x509 -noout -in imapd.pem -subject
```

Display certificate

```
$ openssl x509 -noout -text -in /etc/apache2/ssl/server2016.crt
```

Create key

```
$ openssl genrsa 2048 > www.linuxia.de.key
```

Create certificate request from existing key (SHA2)

```
$ openssl req -new -key www.linuxia.de.key -sha256 -out server2016.csr
```

Create certificate request from existing certificate and key

```
$ openssl x509 -x509toreq -in www.linuxia.de.crt -out www.linuxia.de.csr
-signkey www.linuxia.de.key
```

Show public key for private key

```
$ openssl rsa -in www.linuxia.de.key -pubout
```

Convert certificates to PEM format

```
$ openssl x509 -inform der -in linuxia.crt -out linuxia.pem
```

Test SSL connection and print out SSL certificate

```
$ openssl s_client -connect  192.168.26.241:443
```

Connect to SMTP server with STARTTLS

```
$ openssl s_client -connect  192.168.26.241:25 --starttls smtp
```

Remove passphrase from private key

```
$ openssl rsa -in www.linuxia.de.pass.key -outform PEM -pubout -out www.linuxia.de.key
```

HOWTO

For more information, check the OpenSSL Command-Line HOWTO.

Linuxia Wiki

Stefan Hornburg (Racke)
OpenSSL Usage

wiki.linuxia.de