PKI на OpenSSL

Fix Me!

PKI (Public Key Infrastructure) — инфраструктура открытых ключей.

Реализация инфраструктуры открытых ключей на OpenSSL.

Программа для работы с ключами: XCA

Собственный Удостоверяющий центр (УЦ)

Создание корневого ключа шифрования

```
openssl genrsa -out domain_rootCA.key 4096
```

Создание сертификата корневого ключа без пароля

```
openssl req \
 -new -x509 -days 5000\
  -subj  '/CN=Organization/emailAddress=pki@domain.ru/OU=Organization/O=Organization/L=Yoshkar-Ola/ST=Mari  El/C=RU'\
 -key domain_rootCA.key\
 -out domain_rootCA.crt
```

Создание сертификата корневого ключа с паролем

```
openssl req \
 -new -x509 -days 5000\
  -subj  '/CN=Organization/emailAddress=pki@domain.ru/OU=Organization/O=Organization/L=Yoshkar-Ola/ST=Mari  El/C=RU'\
 -keyout domain_rootCA.key\
 -out domain_rootCA.crt
```

Изменение/создание пароля

```
openssl rsa -des3 -in domain_rootCA.key -out new_domain_rootCA.key
mv new_domain_rootCA.key domain_rootCA.key
```

Удаление пароля

Для того, чтобы удалить пароль нужно его знать!

```
openssl rsa -in domain_rootCA.key -out new_domain_rootCA.key
mv new_domain_rootCA.key domain_rootCA.key
```

Примеры использования

Создание ключа и сертификата для HTTPS

Можно использовать для Apache

```
# Создание ключа шифрования
openssl genrsa -out domain.ru.key 2048

# Создание запроса на сертификат
openssl req -new\
  -subj  '/CN=*.domain.ru/emailAddress=pki@domain.ru/OU=IT/O=Organization/L=Yoshkar-Ola/ST=Mari
El/C=RU'\
 -out domain.ru.csr\
 -key domain.ru.key

# Подписание запрос на сертификат корневым сертификатом
openssl x509 -req\
 -CA domain_rootCA.crt\
 -CAkey domain_rootCA.key\
 -CAcreateserial\
 -in domain.ru.csr\
 -out domain.ru.crt\
 -days 1000
```

Dovecot

Fix Me!

Dovecot

/etc/dovecot/conf.d/10-auth.conf

```
disable_plaintext_auth = yes
auth_mechanisms = plain login
```

/etc/dovecot/conf.d/10-ssl.conf

```
ssl = yes
ssl_cert = </etc/ssl/certs/domain.ru.crt
ssl_key = </etc/ssl/private/domain.ru.key
```

/etc/dovecot/conf.d/10-master.conf

```
service imap-login {
  inet_listener imap {
    port = 143
  }
  inet_listener imaps {
    port = 993
    ssl = yes
  }
}
```

Postfix

Postfix

Fix Me!

/etc/dovecot/conf.d/10-master.conf

```
  unix_listener /var/spool/postfix-o/private/auth {
```

```
    mode = 0666
  }
```

/etc/postfix/postfix-o/main.cf

```
smtpd_use_tls = yes
smtpd_tls_cert_file = /etc/ssl/certs/domain.ru.crt
smtpd_tls_key_file = /etc/ssl/private/domain.ru.key
#smtpd_tls_CApath = /etc/ssl/certs
smtpd_tls_CApath = /etc/ssl/certs/rootCA.crt
smtpd_tls_loglevel = 2
smtpd_tls_received_header = yes
```

/etc/postfix/postfix-o/master.cf

```
smtps     inet  n       -       -       -       -       smtpd
  -o syslog_name=postfix-o/smtps
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_sasl_type=dovecot
  -o smtpd_sasl_path=private/auth
  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
  -o mynetworks=0.0.0.0/0
```

Добавление корневого сертификата УЦ

Для того, чтобы доверять сертификатам, выданным УЦ - нужно оказать доверие корневому сертификата УЦ.

- Firefox
- Google Chrome
- Для программ которые используют общую БД MS Windows, например Google Chrome.

Ссылки

wikipedia: Инфраструктура_открытых_ключей

wikipedia: Самозаверенный сертификат

Своё Certificate Authority — в 5 OpenSSL команд

Свой собственный УЦ на OpenSSL

Создаем сертификаты: OpenSSL

OpenLDAP и Ubuntu на практике > Настройка TLS (Transport Layer Security)

wiki.val.bmstu.ru: Пакет OpenSSL

Советы и трюки по работе с OpenSSL

SSL. Часть 2. Центр сертификации своими руками

Создаём собственный CA и подписываем им сертификаты для своих ресурсов

Практическое руководство по созданию центра сертификации

OpenCA Labs

Как и зачем мы делаем TLS в Яндексе

Что такое TLS

https://ru.wikipedia.org/wiki/STARTTLS

http://wiki2.dovecot.org/SSL

 **Creating a Certificate Authority (CA)**

https://help.ubuntu.com/community/OpenSSL

http://www.alvestrand.no/objectid/2.5.29.31.html

Bog BOS: Безопасность: Сертификаты

Руководство по выживанию — TLS/SSL и сертификаты SSL (X.509)

OpenSSL PKI Tutorial v1.1

http://sysadminmosaic.ru/pki_openssl/pki_openssl

2019-07-15 11:46