

MikroTik Certified Security Engineer

MTCSE

Chapter 4: CRYPTOGRAPHY

Базовые
понятия

PKI

CERTIFICATES



MTI-GROUP LLC / network academy

V.19-01

Что такое криптография

Греческий термин «криптография» означает «секретный шрифт».

Криптография - это область науки криптологии об обеспечении безопасности данных. Она занимается поисками решений четырех важных проблем безопасности - **конфиденциальности, аутентификации, целостности и контроля участников** взаимодействия.

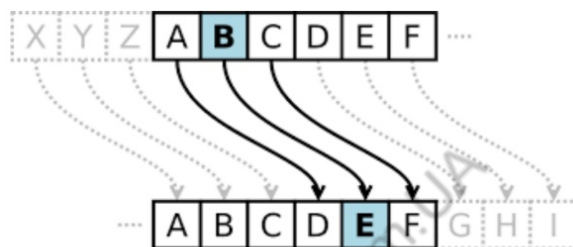
Криптосистема работает по определенной методологии (процедуре). Она состоит из :

- одного или более алгоритмов шифрования (математических формул);
- ключей, используемых этими алгоритмами шифрования;
- системы управления ключами;
- незашифрованного текста;
- и зашифрованного текста (шифротекста).

Квадрат Полибия

	1	2	3	4	5
1	Α	Β	Γ	Δ	Ε
2	Ζ	Η	Θ	Ι	Κ
3	Λ	Μ	Ν	Ξ	Ο
4	Π	Ρ	Σ	Τ	Υ
5	Φ	Χ	Ψ	Ω	

Шифр Цезаря



Скитала древней Спарты



Механизмы безопасности

- **Шифрование:**

- Процесс преобразования открытого текста в зашифрованный текст с использованием криптографического ключа.
- На уровне приложений (Application Layer)- используется для защищенной электронной почты, сеансов базы данных и обмена сообщениями.
- На уровне сеансов (Session layer) - используется Secure Socket Layer (SSL) или Transport Layer Security (TLS)
- На сетевом уровне - использование протоколов, таких как IPsec

Преимущества хорошего алгоритма шифрования:

- Устойчивость к криптографической атаке
- Переменная длина ключа и масштабируемость
- Нет ограничений на экспорт или импорт

Термины

- **plaintext (P)** : оригинальное сообщение
- **ciphertext (C)**: закодированное сообщение
- **cipher** : алгоритм преобразования открытого текста в зашифрованный текст
- **key (k)** : информация, используемая в шифре, известна только отправителю / получателю
- **encipher/encrypt (e)** : преобразование открытого текста в зашифрованный текст
- **decipher/decrypt (d)** : восстановление открытого текста из зашифрованного
- **cryptography** : изучение принципов / методов шифрования
- **cryptanalysis** : изучение принципов / методов расшифровки зашифрованного текста без знания ключа
- **cryptology** : область как криптографии, так и криптоанализа

- **Секретность данных**
- Проверка целостности данных
- Проверка подлинности

Симметричное шифрование

Используется один ключ, с помощью которого производится как шифрование, так и расшифровка с использованием одного и того же алгоритма симметричного шифрования.

Этот ключ передается двум участникам взаимодействия безопасным образом до передачи зашифрованных данных.

- Также известен как алгоритм секретного ключа.



Symmetric Key Algorithms

Symmetric key algorithm	Key size
DES (Data Encryption Standard)	56-bit Keys
3DES (Triple Data Encryption Standard)	112-bit and 168-bit keys
AES (Advanced Encryption Standard)	128, 192, and 256-bit keys
IDEA	128-bit keys
RC2	40 and 64-bit keys
RC4	1 to 256-bit keys
RC5	0 to 2040-bit keys
RC6	128, 192, and 256-bit keys
Blowfish	32 to 448-bit keys

Advanced Encryption Standard (**AES**) - один из наиболее часто используемых и наиболее безопасных алгоритмов шифрования, доступных сегодня.

Замена стареющему стандарту DES.

Явные преимущества:

- блочное шифрование, а не поточное
- значительная длина ключа 256 бит vs 56 бит

Key Size	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2×10^9
56-bit (DES)	7.2×10^{16}
64-bit	1.8×10^{19}
128-bit (AES)	3.4×10^{38}
192-bit (AES)	6.2×10^{57}
256-bit (AES)	1.1×10^{77}

Key size	Time to Crack
56-bit	399 seconds
128-bit	1.02×10^{18} years
192-bit	1.872×10^{37} years
256-bit	3.31×10^{56} years

40-разрядные симметричные ключи весьма ненадежны, для них время полного перебора на высокопроизводительном компьютере оценивается минутами. Рекомендуется использовать 128-разрядные ключи

Симметричные системы обладают самой высокой скоростью шифрования и расшифровки. Однако в симметричных системах есть большая проблема: две стороны должны как-то договориться о ключе шифрования. **Эта проблема известна как задача распределения ключей.**

Основные моменты криптографии:



- Секретность данных
- **Проверка целостности данных**
- Проверка подлинности

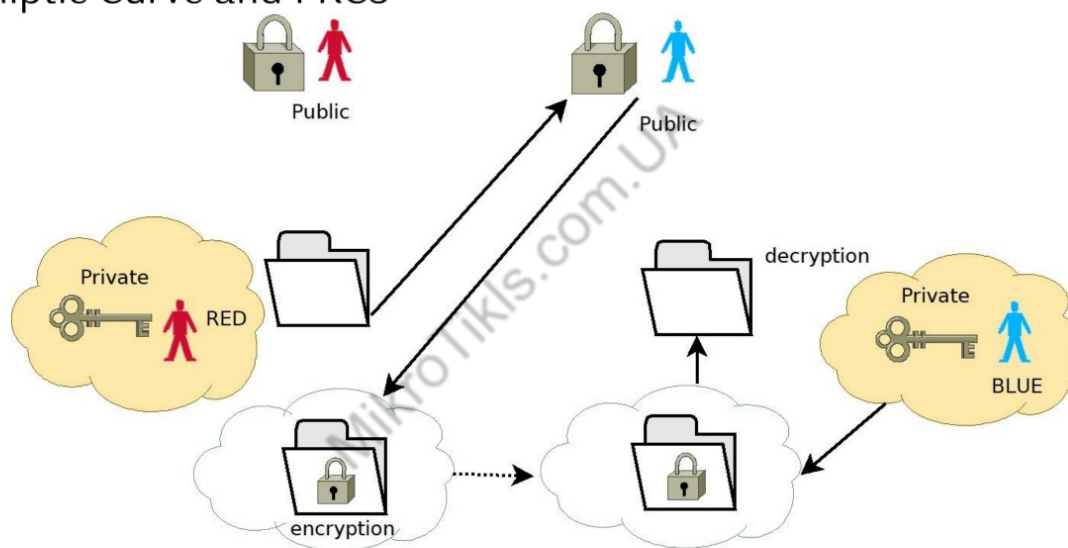
Хэш-функция преобразует большой объем данных в маленький хэш-дайджест (128 или 160 бит)

Обычно применяются следующие хэш-функции:

- MD2, MD5 - разработаны компанией RSA Data Security, создают 128-разрядные дайджесты;
- SHA1,2 - разработанная NIST (Национальным институтом стандартов и технологий США), создает 160-разрядные хэши.

Асимметричное шифрование

- Также называется криптографией с открытым ключом.
- Каждый может видеть открытый ключ.
- Отдельные ключи для шифрования и дешифрования (пары открытого и секретного ключей (512, 1024 или 2048 бит)).
- Примеры алгоритмов асимметричного ключа: RSA, Rivest, Shamir, Adleman, DSA, Diffie-Hellman, El Gamal, Elliptic Curve and PKCS



Асимметричное шифрование

RSA-первая и до сих пор самая распространенная реализация, названа по именам ее создателей: Ривеста, Шамира и Адельмана, основателей компании RSA Data Security

DSA-указанный в стандарте цифровой подписи (DSS) NIST, обеспечивает возможность цифровой подписи для аутентификации сообщений

Diffie-Hellman-используется только для обмена секретными ключами, а не для аутентификации или цифровой подписи

ElGamal-похож на Diffie-Hellman и используется для обмена ключами

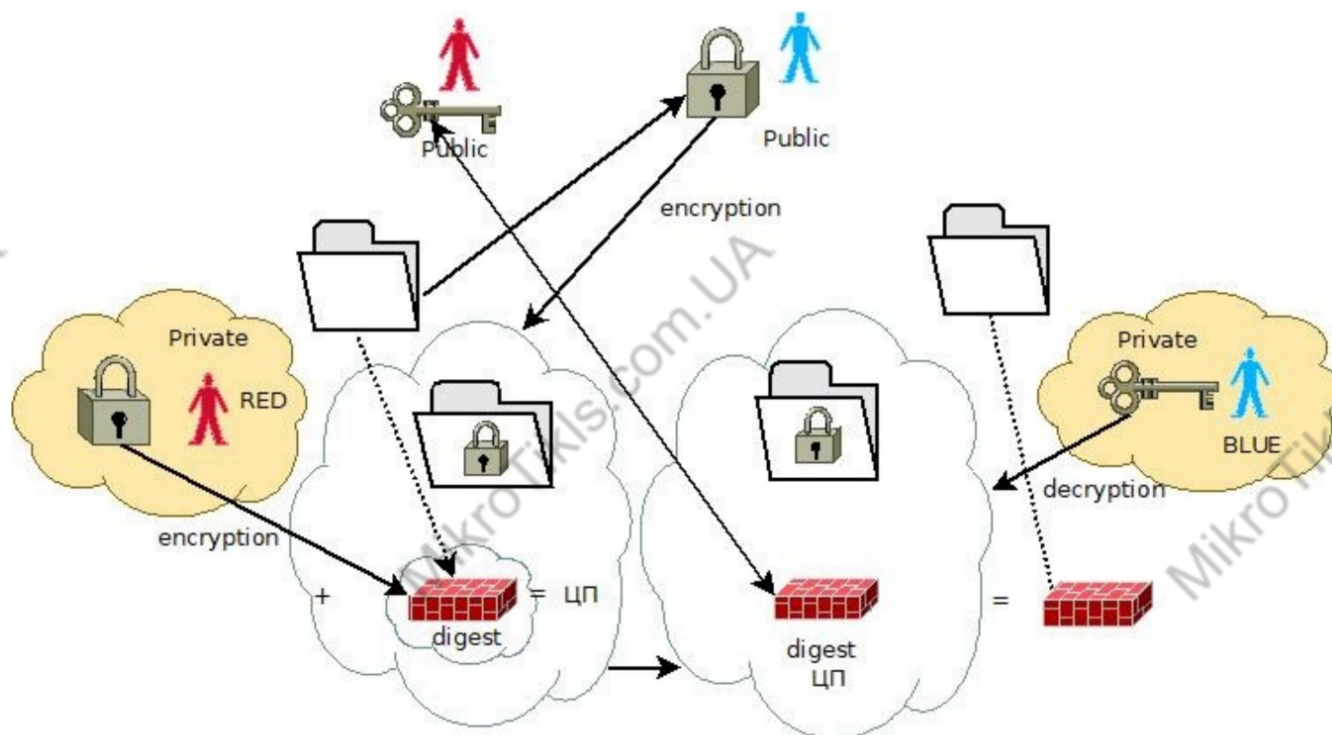
PKCS-набор совместимых стандартов и руководств

Существенный недостаток криптографических систем с открытым ключом - их очень низкая скорость (на два-три порядка ниже, чем у систем симметричного шифрования), поэтому они не годятся для шифрования больших объемов данных

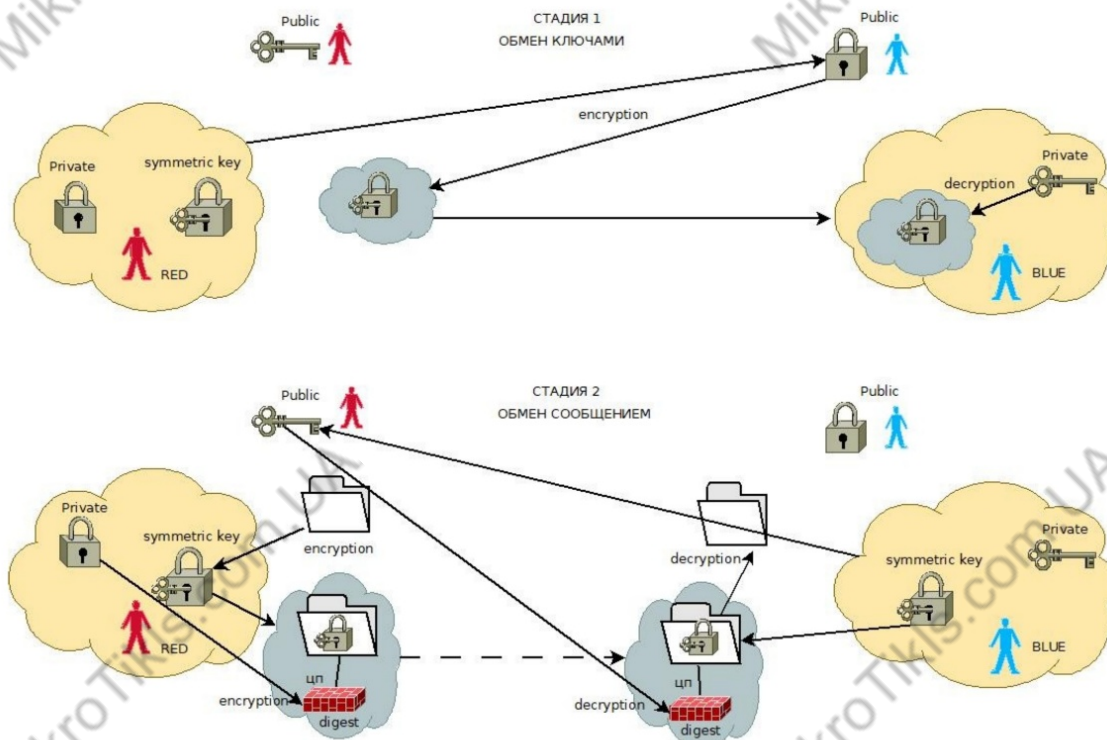
Цифровая подпись

Подписание данных - процедура, объединяющая две криптографические технологии: асимметричное шифрование и хэширование.

- Секретность данных
- Проверка целостности данных
- **Проверка подлинности**



Шифрование сеансовым ключом



симметричная криптография
обеспечивает секретность данных
хэширование
- их целостность,
асимметричная криптография
гарантирует подлинность
данных
и служит для обмена ключами.

Остается решить последнюю проблему

MikroTikls.com

MikroTikls.com

MikroTikls.com

MikroTikls.com.UA

MikroTikls.com.UA

MikroTikls.com.UA

Tikls.com.UA

Tikls.com.UA

Tikls.com.UA

MikroTikls.com

MikroTikls.com

MikroTikls.com

MikroTikls.com.UA

MikroTikls.com.UA

MikroTikls.com.UA

Tikls.com.UA

Tikls.com.UA

Tikls.com.UA

MikroTik Certified Security Engineer

MTCSE

Chapter 4: CRYPTOGRAPHY

Базовые
понятия

PKI

CERTIFICATES



MTI-GROUP LLC / network academy

V.19-01

Public Key Infrastructure (PKI)

Инфраструктура открытых ключей (ИОК, англ. PKI - Public Key Infrastructure) – набор средств (технических, материальных, людских и т. д.), распределённых служб и компонентов, в совокупности используемых для поддержки криптозадач на основе закрытого и открытого ключей. В основе PKI лежит использование криптографической системы с открытым ключом и несколько основных принципов:

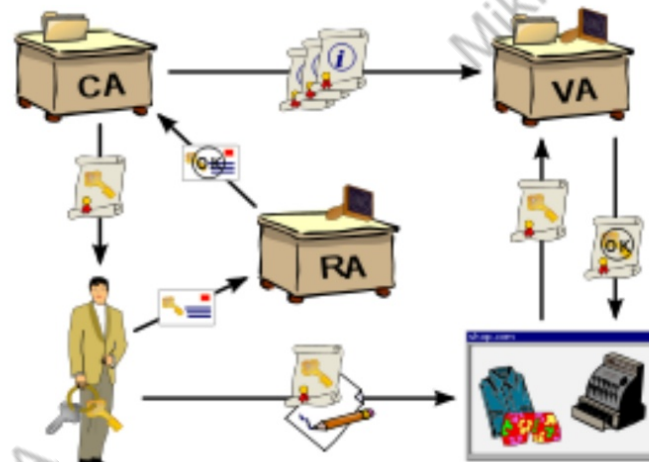
- закрытый ключ (private key) известен только его владельцу;
- удостоверяющий центр создает электронный документ – сертификат открытого ключа, таким образом удостоверяя факт того, что закрытый (секретный) ключ известен эксклюзивно владельцу этого сертификата, открытый ключ (public key) свободно передается в сертификате;
- никто не доверяет друг другу, но все доверяют удостоверяющему центру;
- удостоверяющий центр подтверждает или опровергает принадлежность открытого ключа заданному лицу, которое владеет соответствующим закрытым ключом.

ОСНОВНЫЕ ФУНКЦИИ PKI

- Регистрация
- Инициализация
- Сертификация
- Восстановление пары ключей
- Генерация ключа
- Обновление ключа
- Перекрестная сертификация
- Отзыв

Components of a PKI

- Certificate authority (CA)
- Validation authority (VA)
- Registration authority (RA)
- Central directory



- 1) Пользователь запрашивает сертификат со своим открытым ключом в центре регистрации (RA).
- 2) RA подтверждает личность пользователя в центре сертификации (CA), который, в свою очередь, выдает сертификат.
- 3) Пользователь подписывает какой-либо документ в цифровом виде, используя свой новый сертификат.
- 4) Личность пользователя проверяется договаривающейся стороной с помощью проверяющего органа (VA), который получает информацию о выданных сертификатах от CA.

Отзыв сертификата

- Предположим, что кому-то (или чему-то) сертификат больше не нужен (человек уволился, скомпрометирован секретный ключ и т.п.).
- Срок действия сертификата ещё не кончился, но нужно, чтобы он не работал.
- Для этого администратор СА обновляет список отозванных сертификатов (**Certificate revocation list – далее CRL**) и размещает его в доступном для всех месте

Цепочки сертификатов

Центр сертификации (СА) может делегировать часть своих полномочий подчиненному СА, выдав ему соответствующий сертификат.

Если сертификат конечного пользователя выдан не корневым (Root), а промежуточным СА, проверка такого сертификата превращается в проверку **цепочки сертификатов**

Отзыв сертификата

- Предположим, что кому-то (или чему-то) сертификат больше не нужен (человек уволился, скомпрометирован секретный ключ и т.п.).
- Срок действия сертификата ещё не кончился, но нужно, чтобы он не работал.
- Для этого администратор СА обновляет список отозванных сертификатов (**Certificate revocation list – далее CRL**) и размещает его в доступном для всех месте

Цепочки сертификатов

Центр сертификации (СА) может делегировать часть своих полномочий подчиненному СА, выдав ему соответствующий сертификат.

Если сертификат конечного пользователя выдан не корневым (Root), а промежуточным СА, проверка такого сертификата превращается в проверку **цепочки сертификатов**

Отзыв сертификата

- Предположим, что кому-то (или чему-то) сертификат больше не нужен (человек уволился, скомпрометирован секретный ключ и т.п.).
- Срок действия сертификата ещё не кончился, но нужно, чтобы он не работал.
- Для этого администратор СА обновляет список отозванных сертификатов (**Certificate revocation list – далее CRL**) и размещает его в доступном для всех месте

Цепочки сертификатов

Центр сертификации (СА) может делегировать часть своих полномочий подчиненному СА, выдав ему соответствующий сертификат.

Если сертификат конечного пользователя выдан не корневым (Root), а промежуточным СА, проверка такого сертификата превращается в проверку **цепочки сертификатов**

MikroTik Certified Security Engineer

MTCSE

Chapter 4: CRYPTOGRAPHY

Базовые
понятия

PKI

CERTIFICATES



MTI-GROUP LLC / network academy

V.19-01

Сертификат

- Сертификат - это двоичная структура, содержащая информацию о владельце открытого ключа.
- Самая распространенная форма сертификатов - сертификаты X.509 версий 1, 2 и 3.
- X.509 - это промышленный стандарт сертификатов, определенный в RFC-2459;

Сертификат X.509 :

- номер версии - 1, 2 или 3;
- эмитент - имя эмитента, выпустившего сертификат, обычно в формате X.500;
- серийный номер - числовой идентификатор сертификата, уникальный для данного эмитента;
- срок действия - срок, в течение которого сертификат считается действительным;
- субъект - имя владельца закрытого ключа, парного открытому ключу, содержащемуся в сертификате; как и имя эмитента обычно в формате X.500 ;
- информация об открытом ключе - идентификатор алгоритма асимметричного шифрования, длина ключа и собственно значение открытого ключа;
- алгоритм цифровой подписи - идентификатор алгоритма (точнее пары алгоритмов: хэширования и асимметричного шифрования), используемого для создания цифровой подписи сертификата;
- цифровая подпись сертификата - хэш части содержимого сертификата, зашифрованный закрытым ключом эмитента.

Само значение закрытого ключа в сертификате никогда не присутствует и хранится отдельно.

Основные компоненты имени X.500

Компонент	Описание
C	Страна двумя буквами
S или SP	Штат, область, провинция
L	Населенный пункт
STREET	Адрес в населенном пункте
O	Организация
OU	Отдел в организации
CN	Общее имя
E или Email	Адрес электронной почты

"C=UA, S=Kiev, L=Kiev, O=MTI IT, OU=Software, CN=Pupkin Vasilii Ivanovich, E=pupkin@mti.ua".

CA- Центр Сертификации это:

- Эмитент, подписавший сертификат
- Доверенная (третья) сторона
- На основе модели доверия
- Типы:
 - Корпоративный CA
 - Индивидуальный CA (PGP)
 - Глобальный CA (такой как VeriSign)
- Функции:
 - Регистрация и проверка подписчиков
 - Выдача и управление сертификатами
 - Управление отзывом и возобновлением сертификатов
 - Создание политик и процедур

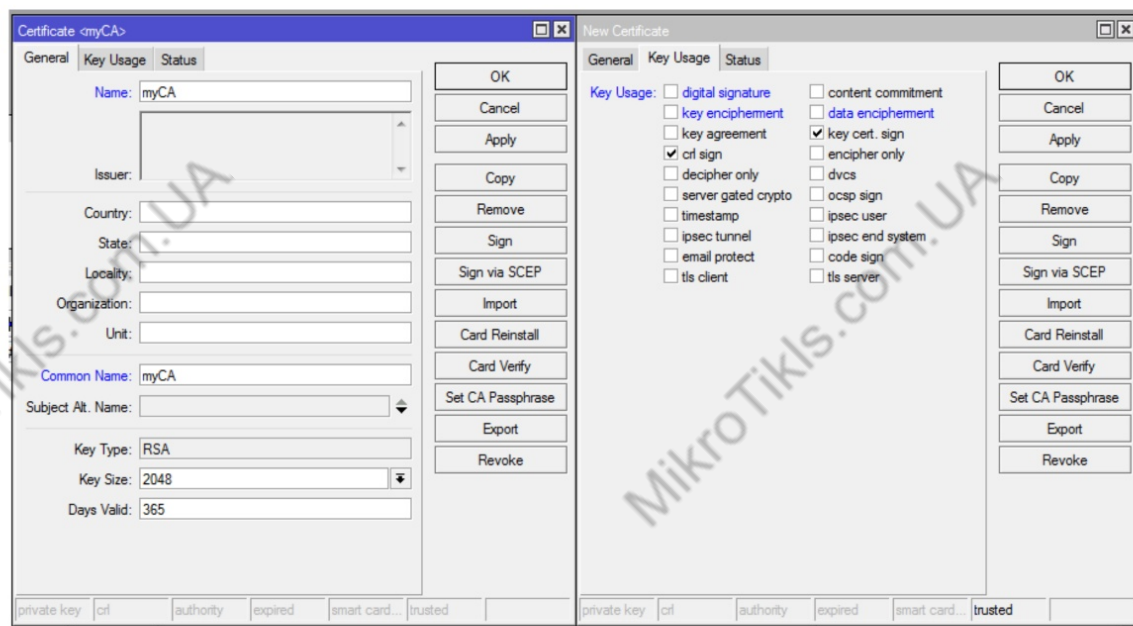
SELF-SIGNED CERTIFICATES

SELF-SIGNED CERTIFICATES

- Самозаверяющий SSL-сертификат не использует цепочку доверия, обычно используемую другими SSL-сертификатами.
- Является подписанным тем же лицом, чью идентификационную информацию он сертифицирует.
- Чаще всего используется, когда компания хочет выполнить внутреннее тестирование без усилий или за счет приобретения стандартного сертификата SSL.

SELF-SIGNED CERTIFICATES on RouterOS

Сначала нам необходимо создать свой собственный СА (центр сертификации), который будет подписывать сертификаты.

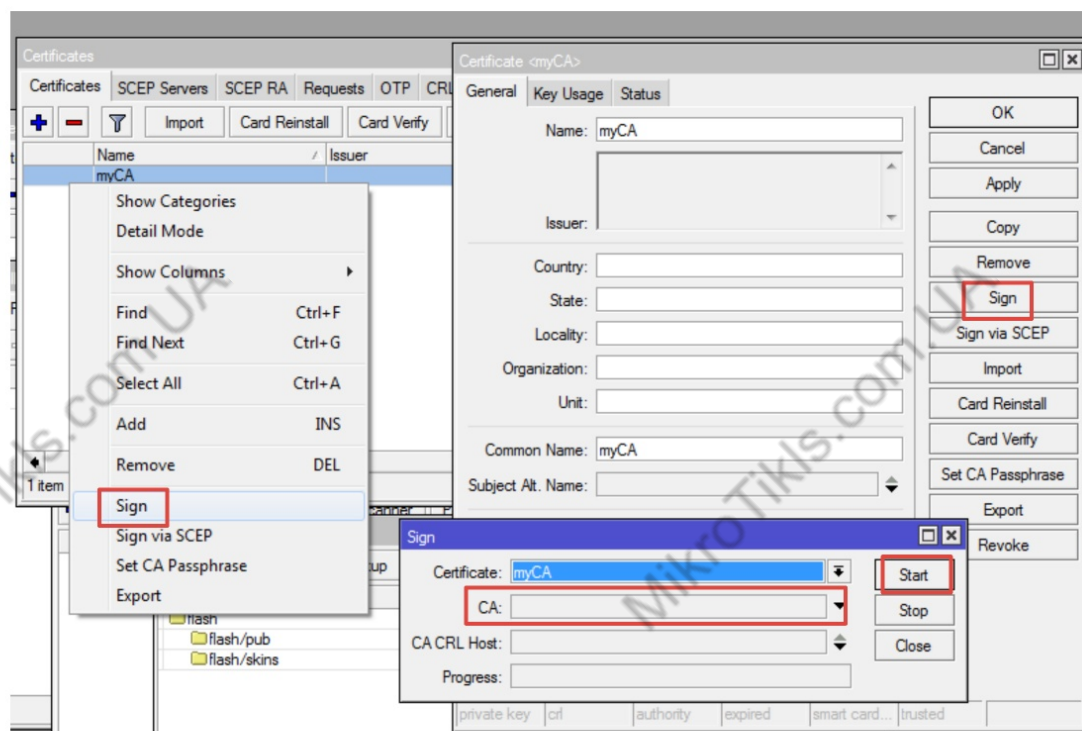


```
/certificate  
add name=myCA  
common-name=myCa  
key-usage=key-cert-sign,crl-sign
```

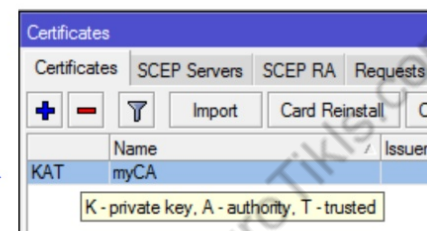
В примере указан минимум требуемых конфигураций. Но на практике, в целях корпоративной или собственной безопасности требуется заполнить все поля по форме X.500

SELF-SIGNED CERTIFICATES on RouterOS

самоподписываем созданную заготовку



/certificate
sign myCa



SELF-SIGNED CERTIFICATES on RouterOS

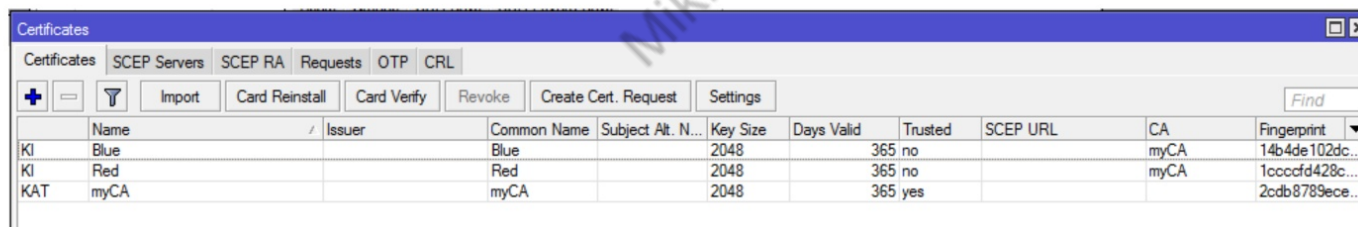
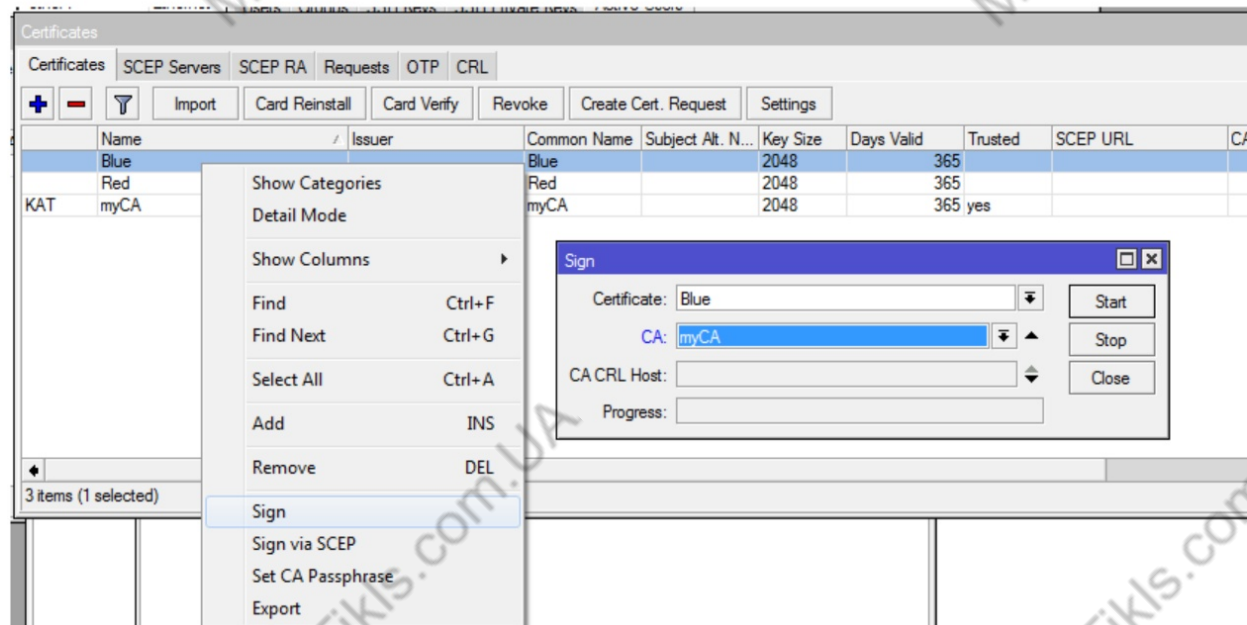
Наша задача
обеспечить
сертификатами
клиентов "Blue" и "Red"

Name	Issuer	Common Name	Subject Alt. N...	Key Size	Days Valid	Trusted	SCEP URL	CA
Blue		Blue		2048	365			
Red		Red		2048	365			
KAT	myCA	myCA		2048	365	yes		

- Создаем две заготовки
- До подписания они не содержат никаких ключей

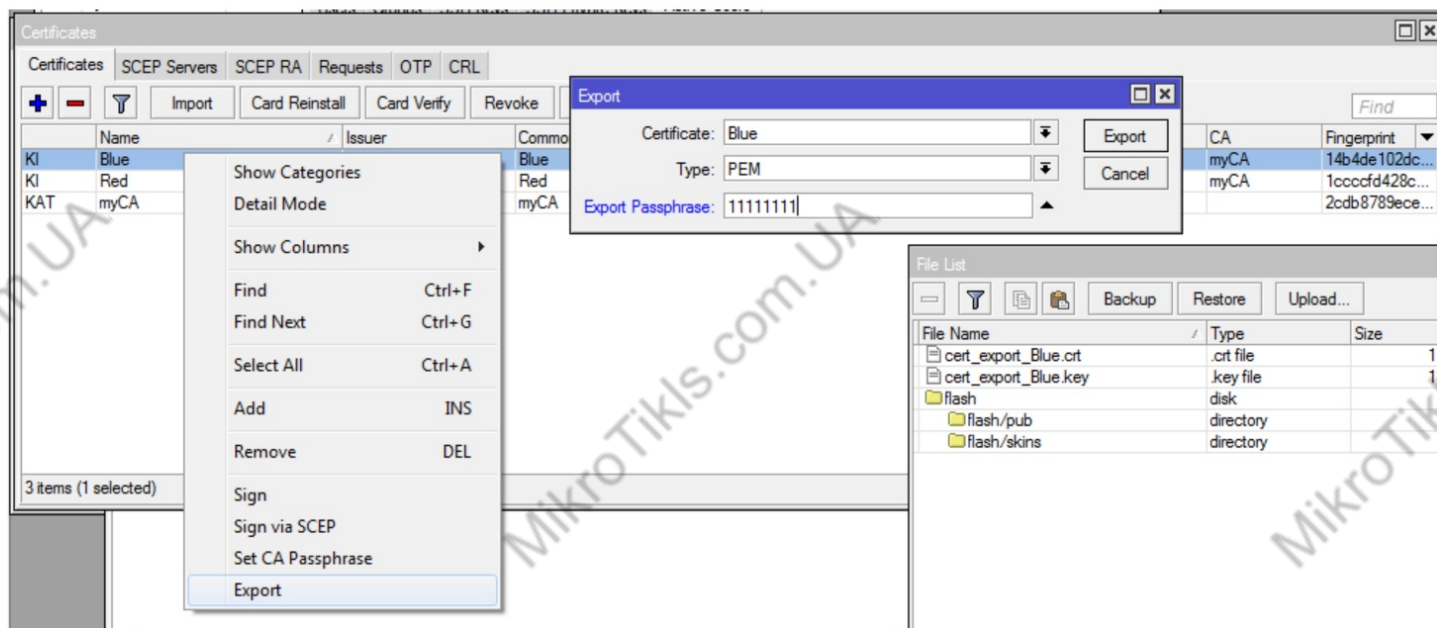
SELF-SIGNED CERTIFICATES on RouterOS

- Подписываем наши заготовки собственным CA
- Теперь это выпущенная пара ключей приватного и публичного



SELF-SIGNED CERTIFICATES on RouterOS

Экспортируем в file list ключи, используя пароль



SELF-SIGNED CERTIFICATES on RouterOS

cert_export_Blue.crt

cert_export_Red.crt
cert_export_Red.key

Router (Red)



cert_export_Red.crt

cert_export_Blue.crt
cert_export_blue.key

Router (Blue)

SELF-SIGNED CERTIFICATES on RouterOS

Импортируем сертификаты на **Router (Blue)**

и

по аналогии на Router(Red)

Import Dialog 1:

Only File: cert_export_Blue.crt

Passphrase:

File List 1:

File Name	Type	Size	Creation
cert_export_Blue.crt	.crt file	1111 B	Sep 11 2011
cert_export_Blue.key	.key file	1858 B	Sep 11 2011
cert_export_Red.crt	.crt file	1111 B	Sep 11 2011

Import Dialog 2:

Only File: cert_export_Blue.key

Passphrase: 11111111

File List 2:

File Name	Type	Size	Creation
cert_export_Blue.crt	.crt file	1111 B	Sep 11 2011
cert_export_Blue.key	.key file	1858 B	Sep 11 2011
cert_export_Red.crt	.crt file	1111 B	Sep 11 2011

Import Dialog 3:

Only File: cert_export_Red.crt

Passphrase:

File List 3:

File Name	Type	Size	Creation
cert_export_Blue.crt	.crt file	1111 B	Sep 11 2011
cert_export_Blue.key	.key file	1858 B	Sep 11 2011
cert_export_Red.crt	.crt file	1111 B	Sep 11 2011

SELF-SIGNED CERTIFICATES on RouterOS

Пример использования в IPSec для метода
аутентификации вместо psk -> digital signature

Router (Blue)

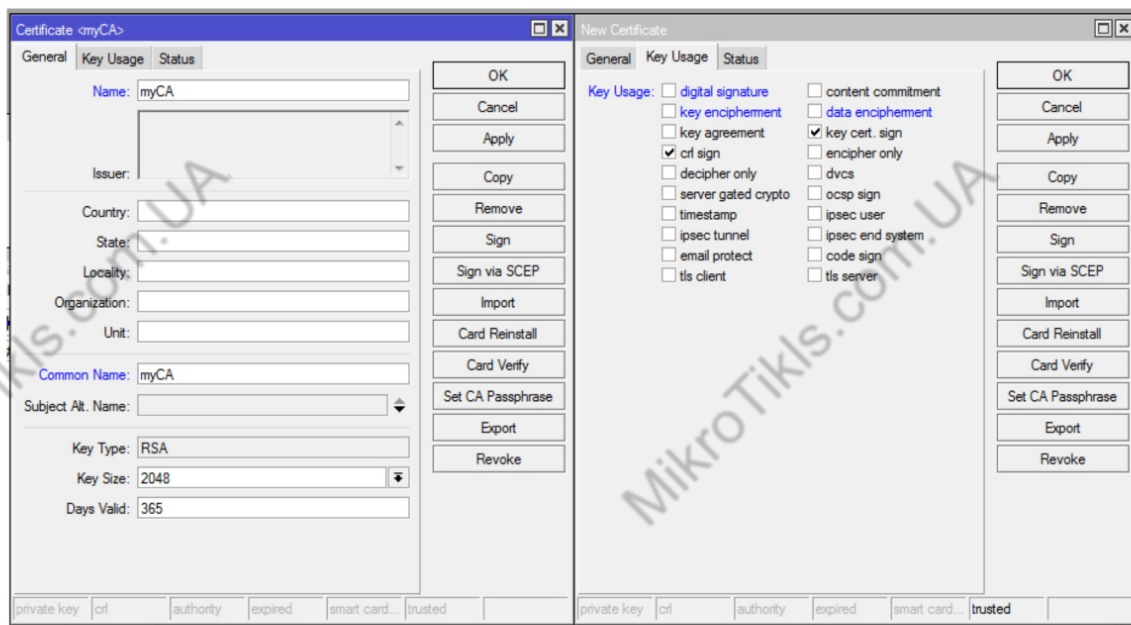
The screenshot shows the 'IPsec Identity <peerRed>' configuration window in RouterOS WinBox. The 'Auth. Method' is set to 'digital signature'. The 'Certificate' is 'cert_export_Blue.crt_0' and the 'Remote Certificate' is 'cert_export_Red.crt_0'. The 'Policy Template Group' is 'default', 'Notrack Chain' is empty, 'My ID Type' is 'auto', 'Remote ID Type' is 'auto', 'Match By' is 'remote id', 'Mode Configuration' is empty, and 'Generate Policy' is 'no'. The status at the bottom is 'enabled'.

Router (Red)

The screenshot shows the 'IPsec Identity <peerBlue>' configuration window in RouterOS WinBox. The 'Auth. Method' is set to 'digital signature'. The 'Certificate' is 'cert_export_Red.crt_0' and the 'Remote Certificate' is 'cert_export_Blue.crt_0'. The 'Policy Template Group' is 'default', 'Notrack Chain' is empty, 'My ID Type' is 'auto', 'Remote ID Type' is 'auto', 'Match By' is 'remote id', 'Mode Configuration' is empty, and 'Generate Policy' is 'no'. The status at the bottom is 'enabled'.

SELF-SIGNED CERTIFICATES on RouterOS for OVPN/SSTP

Сначала нам необходимо создать свой собственный CA (центр сертификации), который будет подписывать сертификаты.

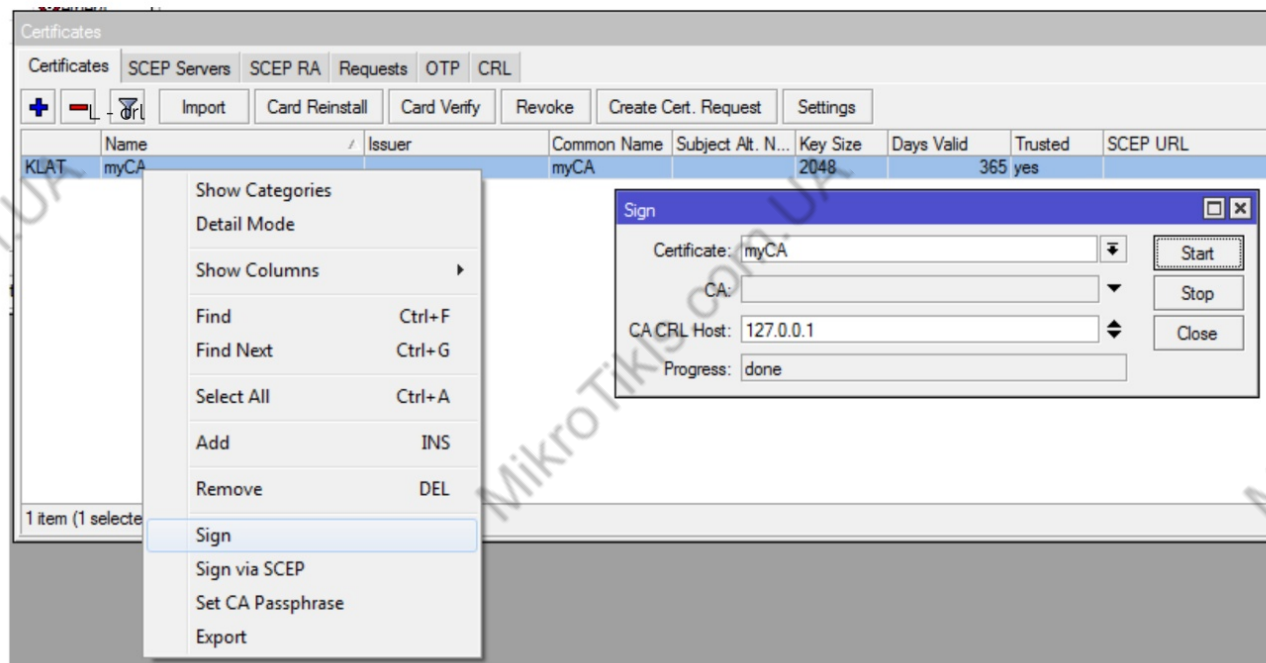


```
/certificate  
add name=myCA  
common-name=myCa  
key-usage=key-cert-sign,crl-sign
```

В примере указан минимум требуемых конфигураций. Но на практике, в целях корпоративной или собственной безопасности требуется заполнить все поля по форме X.500

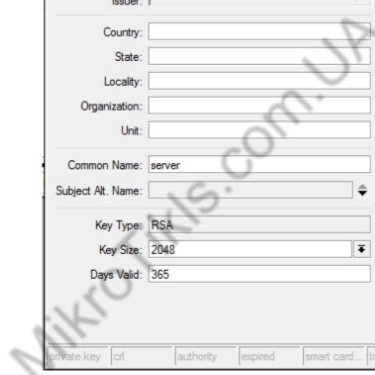
SELF-SIGNED CERTIFICATES on RouterOS for OVPN/SSTP

Самоподписываем заготовку myCA с указанием CA CRL Host для дальнейшего отзыва сертификатов



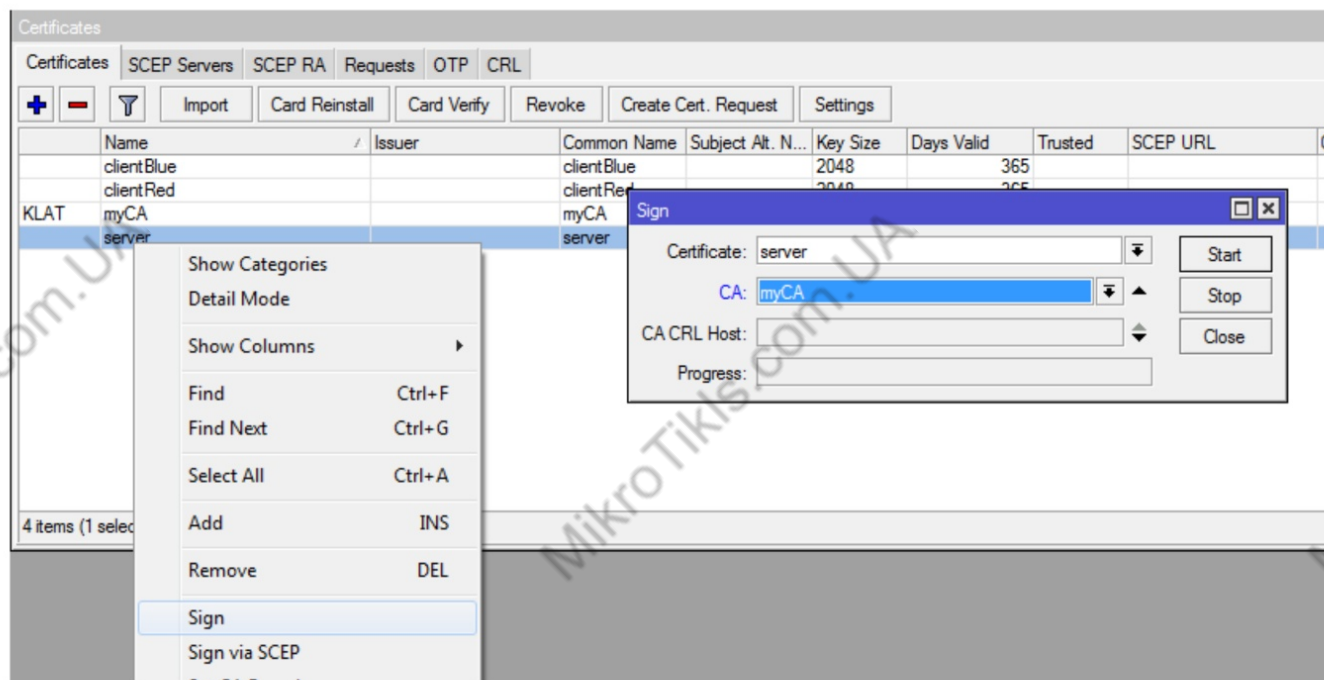
MikroTiks.com

MikroTikIs.com

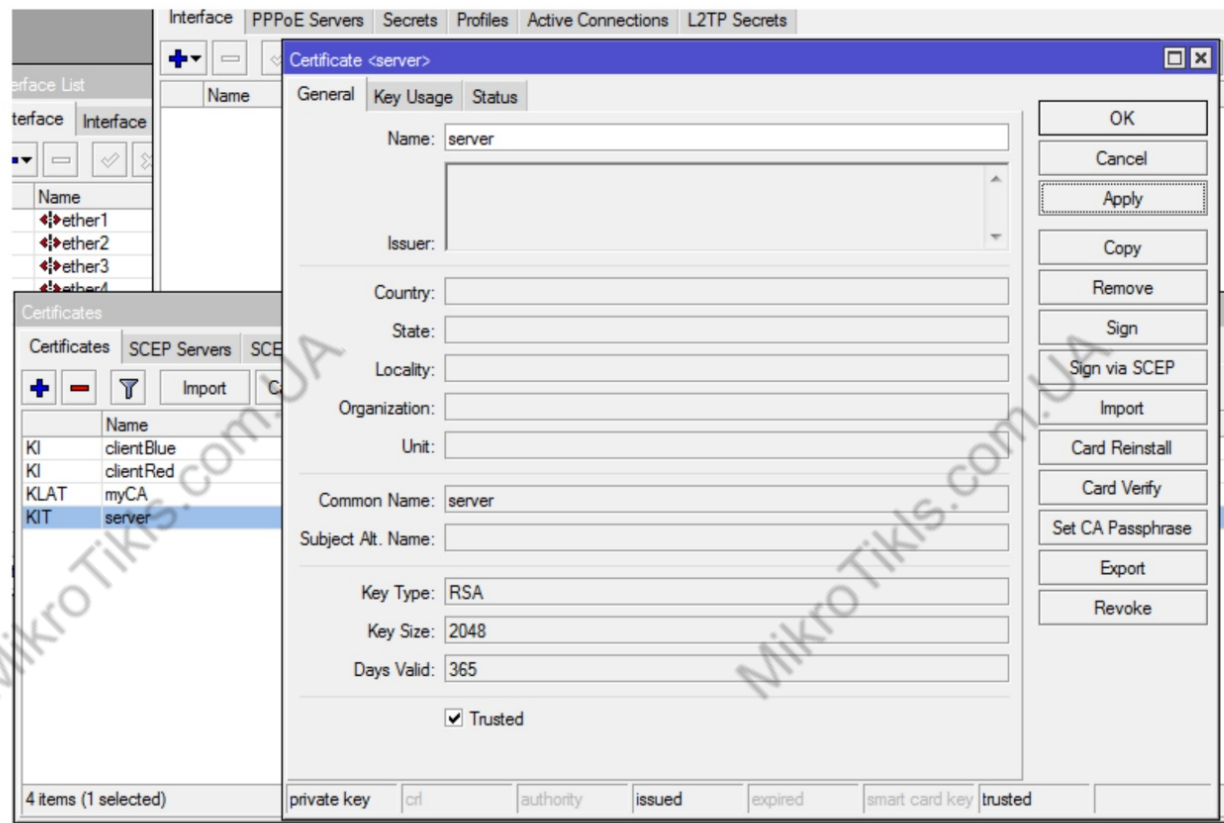


SELF-SIGNED CERTIFICATES on RouterOS for OVPN/SSTP

Подписываем собственным Центром Сертификации (myCA)

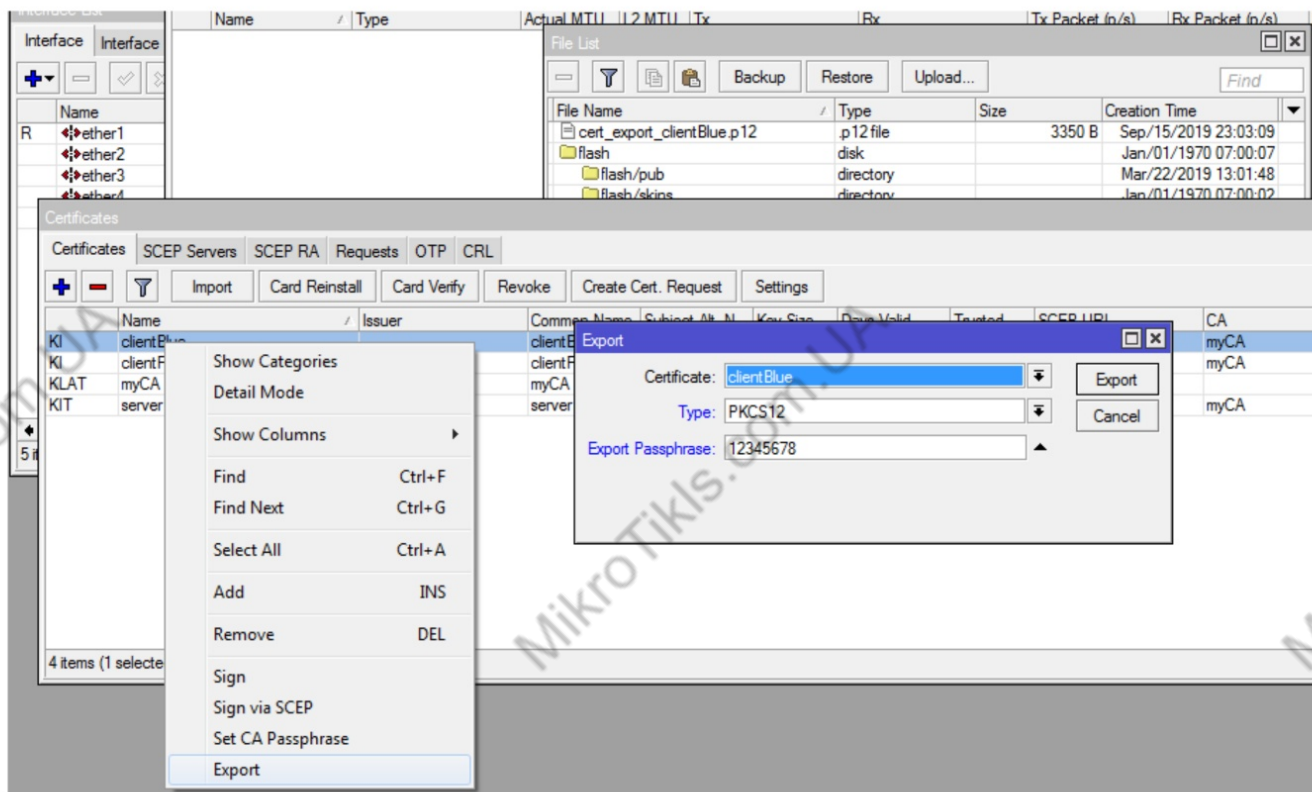


SELF-SIGNED CERTIFICATES on RouterOS for OVPN/SSTP

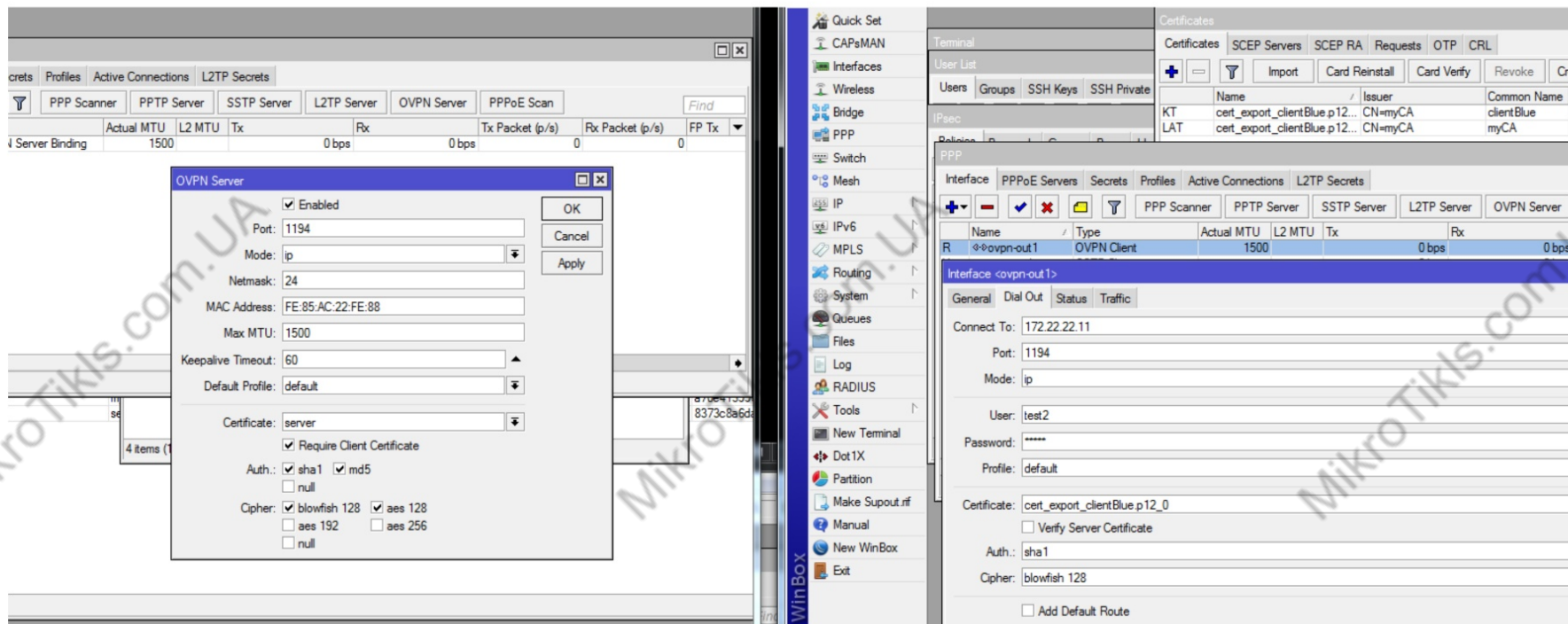


На сервере ставим галочку Trusted, поскольку будем использовать его на этом маршрутизаторе

SELF-SIGNED CERTIFICATES on RouterOS for OVPN/SSTP

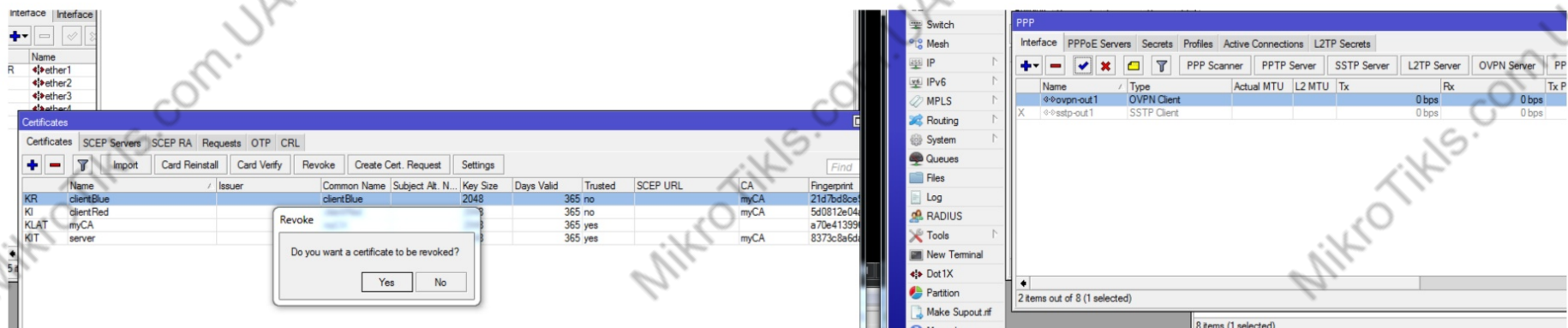


SELF-SIGNED CERTIFICATES on RouterOS for OVPN/SSTP



SELF-SIGNED CERTIFICATES on RouterOS for OVPN/SSTP

При необходимости, myCA может отозвать (Revoke) сертификат клиента



FREE OF CHARGE VALID CERTIFICATES

- Let's Encrypt - это новый центр сертификации (CA), который предлагает БЕСПЛАТНЫЕ SSL-сертификаты, которые так же безопасны, как и текущие платные сертификаты.
- Let's Encrypt - это бесплатный центр сертификации, разработанный Исследовательской группой по безопасности в Интернете (ISRG).
- SSL-сертификаты выдаются сроком на 90 дней, и их необходимо продлить. Эти сертификаты проходят проверку домена, не требуют выделенного IP-адреса и поддерживаются всеми решениями хостинга SiteGround.

<https://www.sslforfree.com/>

sslforfree.com

[Login](#) [Need Help?](#)

SSL For Free

Free SSL Certificates & Free Wildcard SSL Certificates in Minutes

 Secure | <https://tsyapa.com>

[Create Free SSL Certificate](#)



100% Free Forever

Never pay for SSL again. Thanks to [Letsencrypt](#) the first non-profit CA.



Widely Trusted

Our free SSL certificates are trusted in 99.9% of all major browsers.



Enjoy SSL Benefits

- Protect user data & gain trust
- Improve Search Engine Ranking
- Prevent forms of website hacking

Over 3,000,000+ Free SSL Certificates Created With SSLForFree

Free SSL Certificate Validation for "tsyapa.com, www.tsyapa.com"

(Add / Edit Domains | Regenerate Account)

Verify that you own the domain through your web server or if your domain is not yet on a web server then verify it through the DNS. This prevents other people from getting an SSL certificate for your domain. By continuing you agree to the Lets Encrypt service agreement. You may need to whitelist 66.133.109.36 if your website is behind a firewall. If you receive a 504 Gateway timeout and cannot connect anymore then open another incognito/private browser or a different browser to connect again. If you have your own CSR use manual verification and input it after generating domain verification files. If you need further help with verification you can also view tutorials.

Automatic FTP Verification
Enter FTP information to automatically verify the domain

Manual Verification
Upload verification files manually to your domain to verify ownership.

Manual Verification (DNS)
Use this if you cannot verify through a web server or port 80. You will add TXT records to your DNS server.

Manually Verify Domain (HTTP Server)

If you do not have your FTP information then follow the following steps to verify domain ownership manually. The server will need to be on port 80 if HTTP (or port 80 open and forwarding to 443 if HTTPS). If your web server is not listening on port 80 then you will need to temporarily listen on port 80 or forward port 80 to the port for the web server.

1. Get domain verification files by clicking the button below
2. Upload domain verification files to domain (Need help?)
3. Download your **free ssl certificate**

Manually Verify Domain

3. Download your **free ssl certificate**

Retry Manual Verification

Upload Verification Files

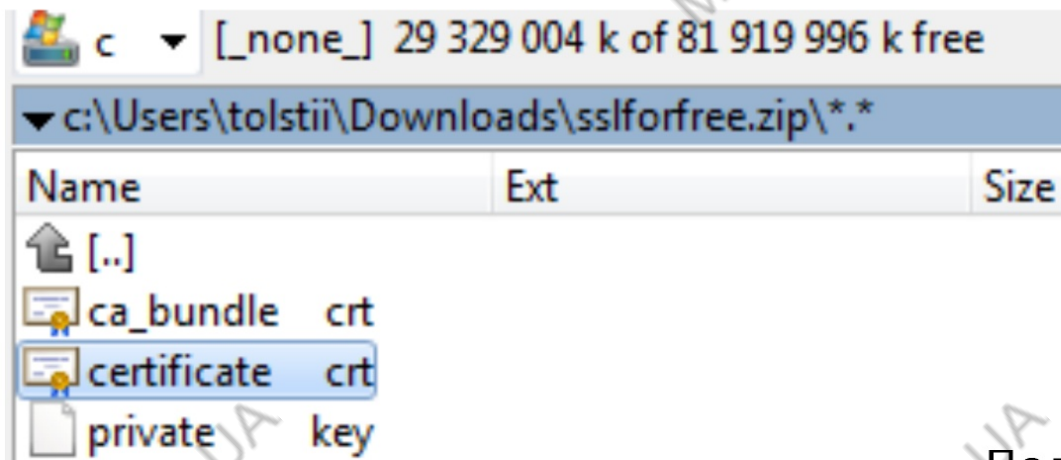
1. Download the following verification files by clicking on each link below

1. Download File #1
2. Download File #2

2. Create a folder in your domain named ".well-known" if it does not already exist. If you use Windows you may have to add a dot at the end of the folder name in order to create a folder with a dot at the beginning.
3. Create another folder in your domain under ".well-known" named "acme-challenge" if it does not already exist
4. Upload the downloaded files to the "acme-challenge" folder
5. Verify successful upload by visiting the following links in your browser
 1. <http://tsyapa.com/.well-known/acme-challenge/YKhYT634e6NXFoQB56S004hgk0IFqtqxql2aJA/vh4>
 2. http://www.tsyapa.com/.well-known/acme-challenge/v6VY9qRjtB3ve0qUnFx6bR4gXOf3FsladmQz_dqESqY
6. If the files do not show random alphanumeric characters or shows an error then recheck that you are uploading in the correct place. Also try viewing the page source (Right-click then click "view page source") of the above links to make sure nothing else shows up but the verification file contents. If you use IIS then you may have to change your server config so that files without an extension (or the wildcard MIME type) serves as text/plain. Contact your host if you are unsure.
7. Click Download SSL Certificate below.

Download SSL Certificate

[illegible][illegible][illegible]



Полученные сертификаты
можете импортировать на
любые свои устройства и
использовать под разные
задачи

Lab

В группе поднимите VPN (OVPN) с использованием сертификатов

Использование самоподписных сертификатов на устройствах под управлением Windows

SSTP (ROS)



SSTP (Windows)

Создаем сертификаты CA и Server, в качестве CN - внешний IP

Certificates

Name	Issuer	Common N...	Subject Alt. N...	Key Size	Days Valid	Trusted
KLAT	CAasp	172.22.22.11		2048	365	yes
KIT	serverSSTP	172.22.22.11		2048	365	yes

Certificate <CAasp>

General Key Usage Status

Name: CAasp

Issuer:

Country: ru

State: ru

Locality: ru

Organization: qtr

Unit: ru

Common Name: 172.22.22.11

Subject Alt. Name:

Key Type: RSA

Key Size: 2048

Days Valid: 365

☒ Trusted

private key crt authority expired smart card key trusted

Certificates

Name	Issuer	Common N...	Subject Alt. N...	Key Size	Days Valid	Trusted
KLAT	CAasp	172.22.22.11		2048	365	yes
KIT	serverSSTP	172.22.22.11		2048	365	yes

Certificate <serverSSTP>

General Key Usage Status

Name: serverSSTP

Issuer:

Country: ru

State: ru

Locality: ru

Organization: qtr

Unit: ru

Common Name: 172.22.22.11

Subject Alt. Name:

Key Type: RSA

Key Size: 2048

Days Valid: 365

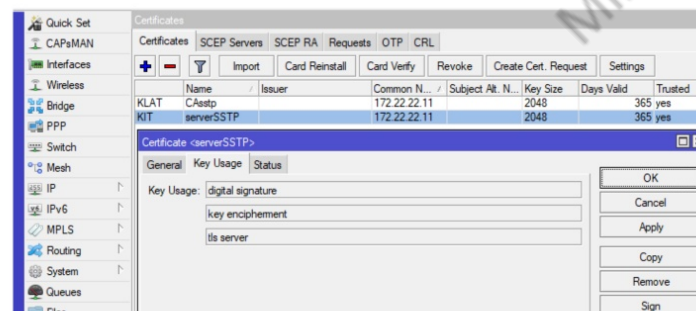
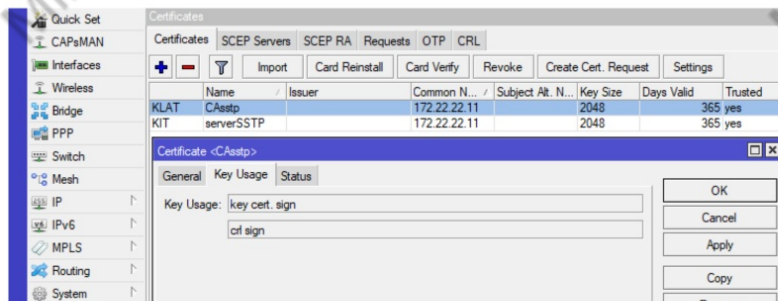
☒ Trusted

private key crt authority issued expired smart card k... trusted

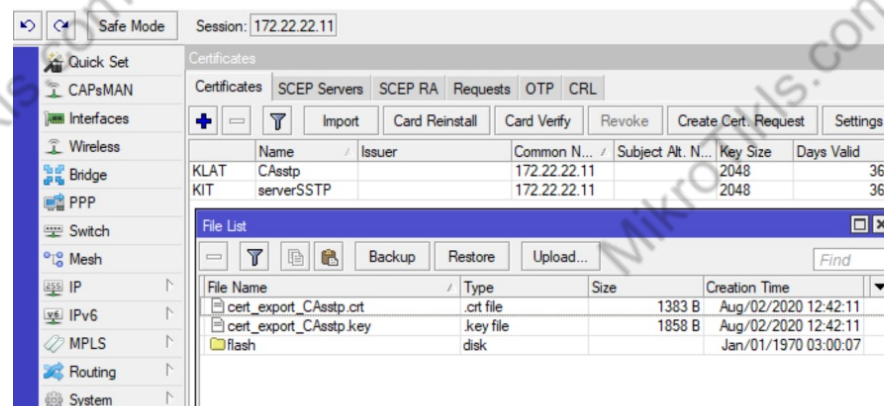
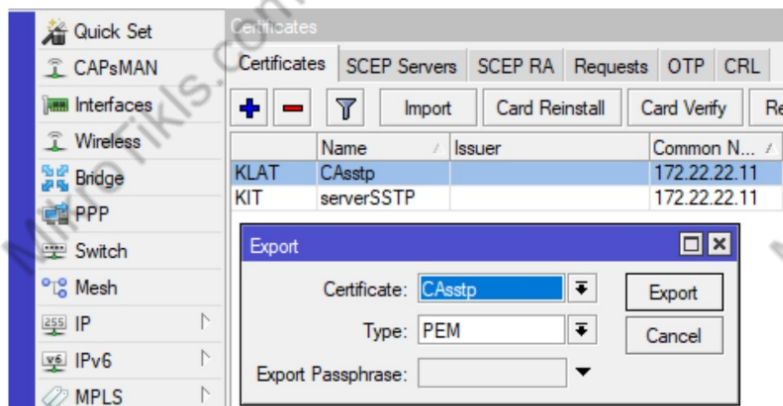
SSTP (ROS)



SSTP (Windows)



Экспортируем CA сертификат типом PEM



SSTP (ROS)



Включаем сервер

PPP

Interface PPPoE Servers Secrets Profiles Active Connections L2TP Secrets

PPP Scanner PPTP Server SSTP Server

Name	Type	Actual MTU	L2 MTU	Tx
------	------	------------	--------	----

SSTP Server

☒ Enabled

Port: 443

Max MTU: 1500

Max MRU: 1500

MRRU:

Keepalive Timeout: 60

Default Profile: default-encryption

Authentication: ☒ mschap2 ☐ mschap1
☐ chap ☐ pap

Certificate: serverSSTP

TLS Version: any

☐ Verify Client Certificate
☐ Force AES
☐ PFS

OK Cancel Apply

SSTP (Windows)

создаем пользователя

PPP

Interface PPPoE Servers Secrets Profiles Active Connections

PPP Authentication&Accounting

Name	Password	Service	Caller ID	Profile
sstpAT	sstpAT	sstp		default-encr

PPP Secret <sstpAT>

Name: sstpAT

Password: sstpAT

Service: sstp

Caller ID:

Profile: default-encryption

Local Address: 192.168.134.1

Remote Address: 192.168.134.2

Remote IPv6 Prefix:

Routes:

Limit Bytes In:

Limit Bytes Out: 0

Last Logged Out: Aug/02/2020 12:44:00

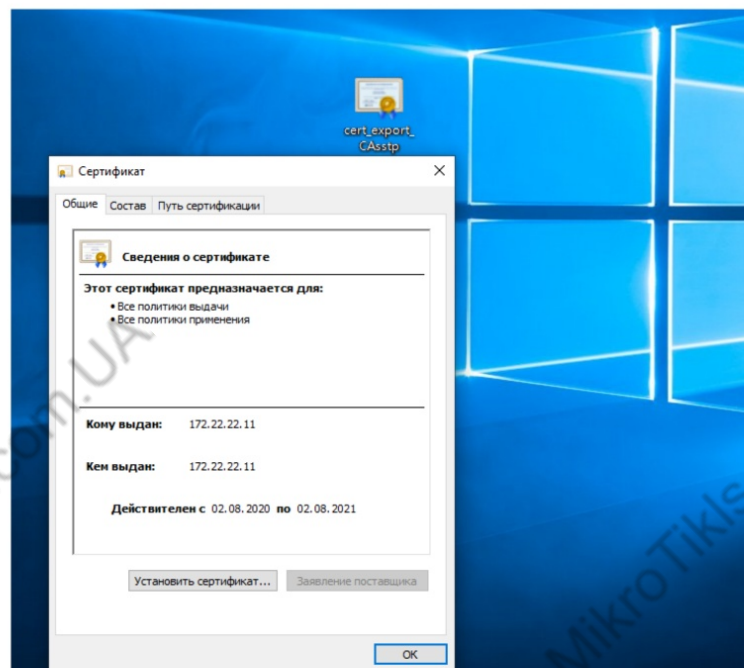
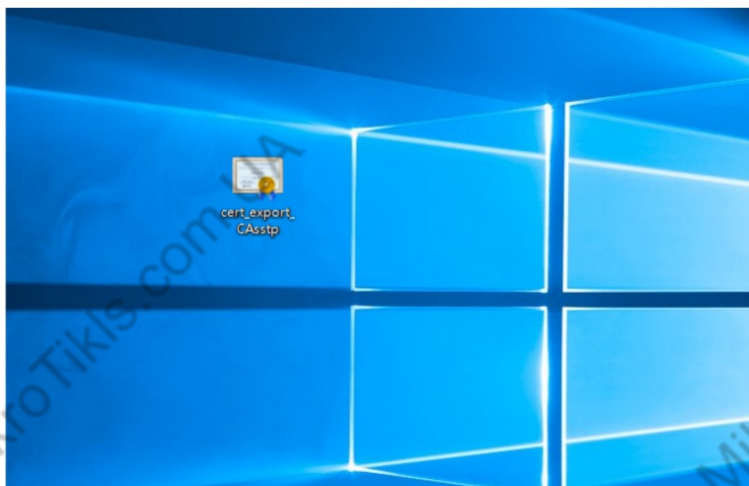
OK Cancel Apply Disable Comment Copy Remove

SSTP (ROS)



SSTP (Windows)

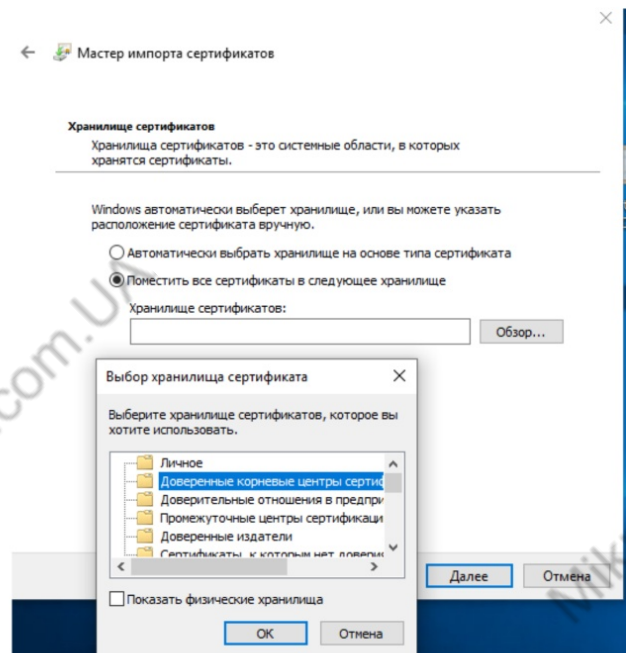
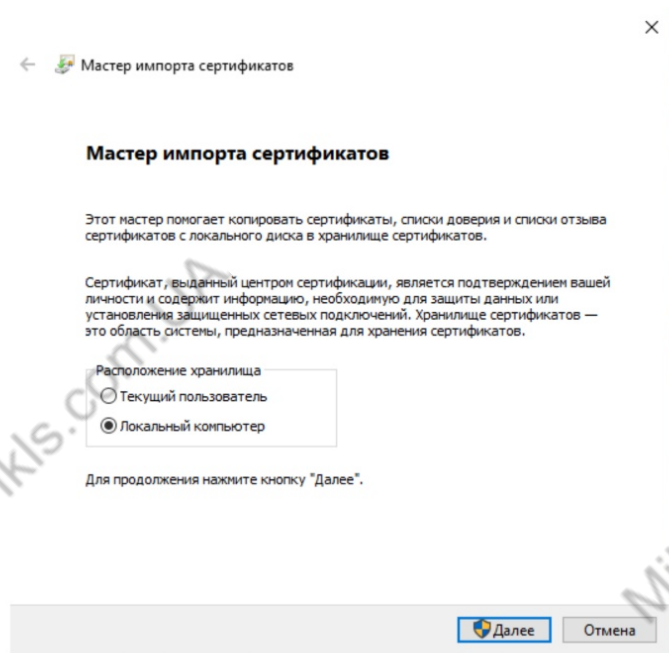
Переносим сертификат на windows и устанавливаем



SSTP (ROS)



SSTP (Windows)



SSTP (ROS)



SSTP (Windows)

← Мастер импорта сертификатов

Завершение мастера импорта сертификатов

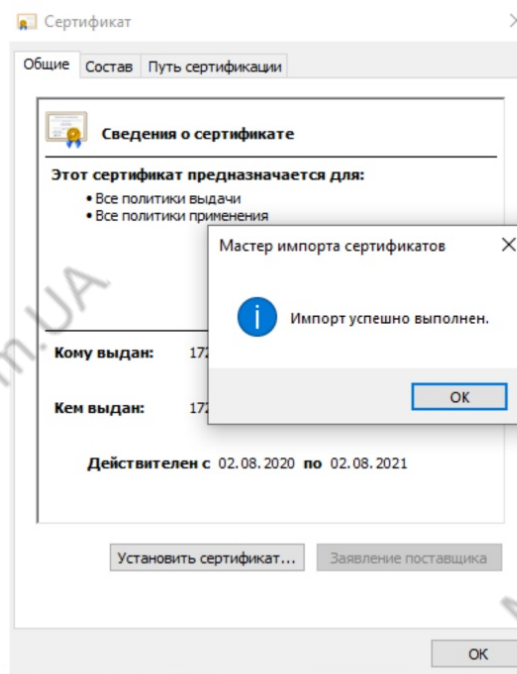
Сертификат будет импортирован после нажатия кнопки "Готово".

Были указаны следующие параметры:

Хранилище сертификатов, выбранное пользователем	Доверенные корневые центры сертификации
Содержимое	Сертификат

Готово

Отмена



SSTP (ROS)



SSTP (Windows)

Настраиваем SSTP подключение на Windows

Добавить VPN-подключение

Поставщик услуг VPN
Windows (встроенные)

Имя подключения
UserX

Имя или адрес сервера
172.22.22.11

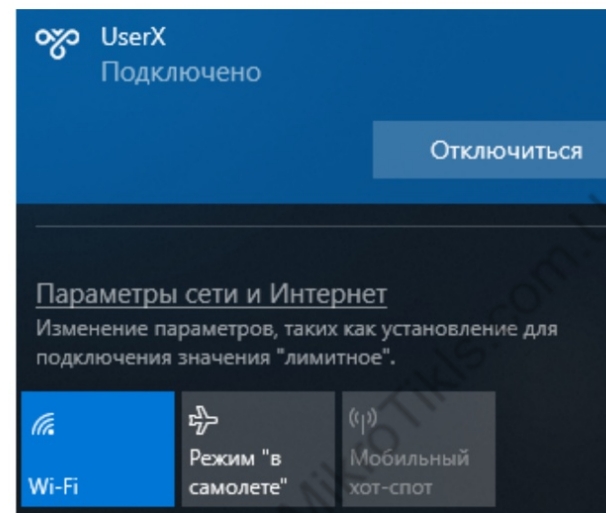
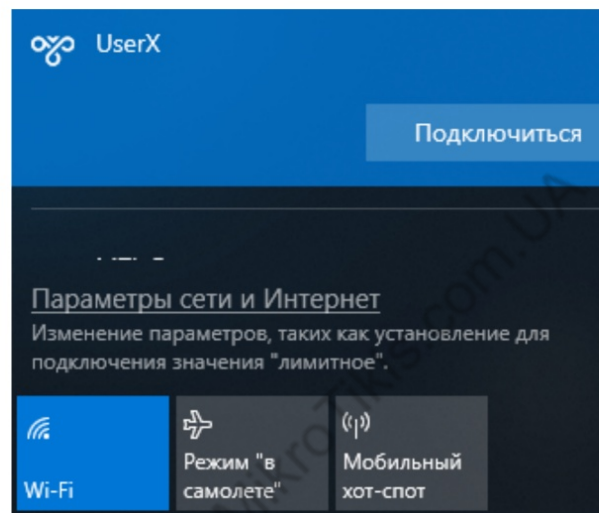
Тип VPN
Протокол SSTP

Тип данных для входа
Имя пользователя и пароль

Имя пользователя (необязательно)
sstpAT

Пароль (необязательно)
•••••

☒ Запомнить мои данные для входа



MikroTik Certified Security Engineer

MTCSE

Chapter 4: CRYPTOGRAPHY

Базовые
понятия

PKI

CERTIFICATES



MTI-GROUP LLC / network academy

V.19-01