

A background image of a businessman in a suit holding several large, metallic, interlocking gears. The scene is in a professional office setting with blurred background elements like a window and a desk.

Настройка и основные возможности ViPNet TLS Gateway.

Отдел технического сопровождения ОАО
«ИнфоТеКС»

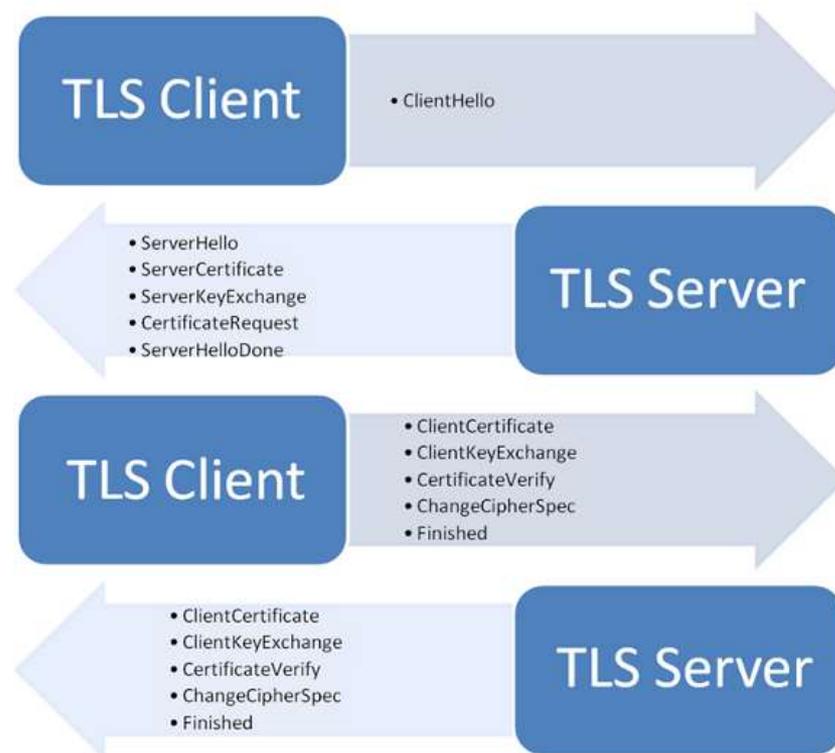
План вебинара:

- Краткое описание протокола TLS/SSL
- Назначение и основные возможности ViPNet TLS Gateway
- Инициализация и настройка ViPNet TLS Gateway
 - Подготовка к работе
 - Развертывание TLS Gateway VA
 - Активация лицензии
 - Первичная инициализация
 - Подготовка рабочего места Администратора и пользователя для подключения к Web-интерфейсу
 - Работа с Web-интерфейсом
 - Типовые вопросы и ошибки при настройке ViPNet TLS Gateway
- Вопросы

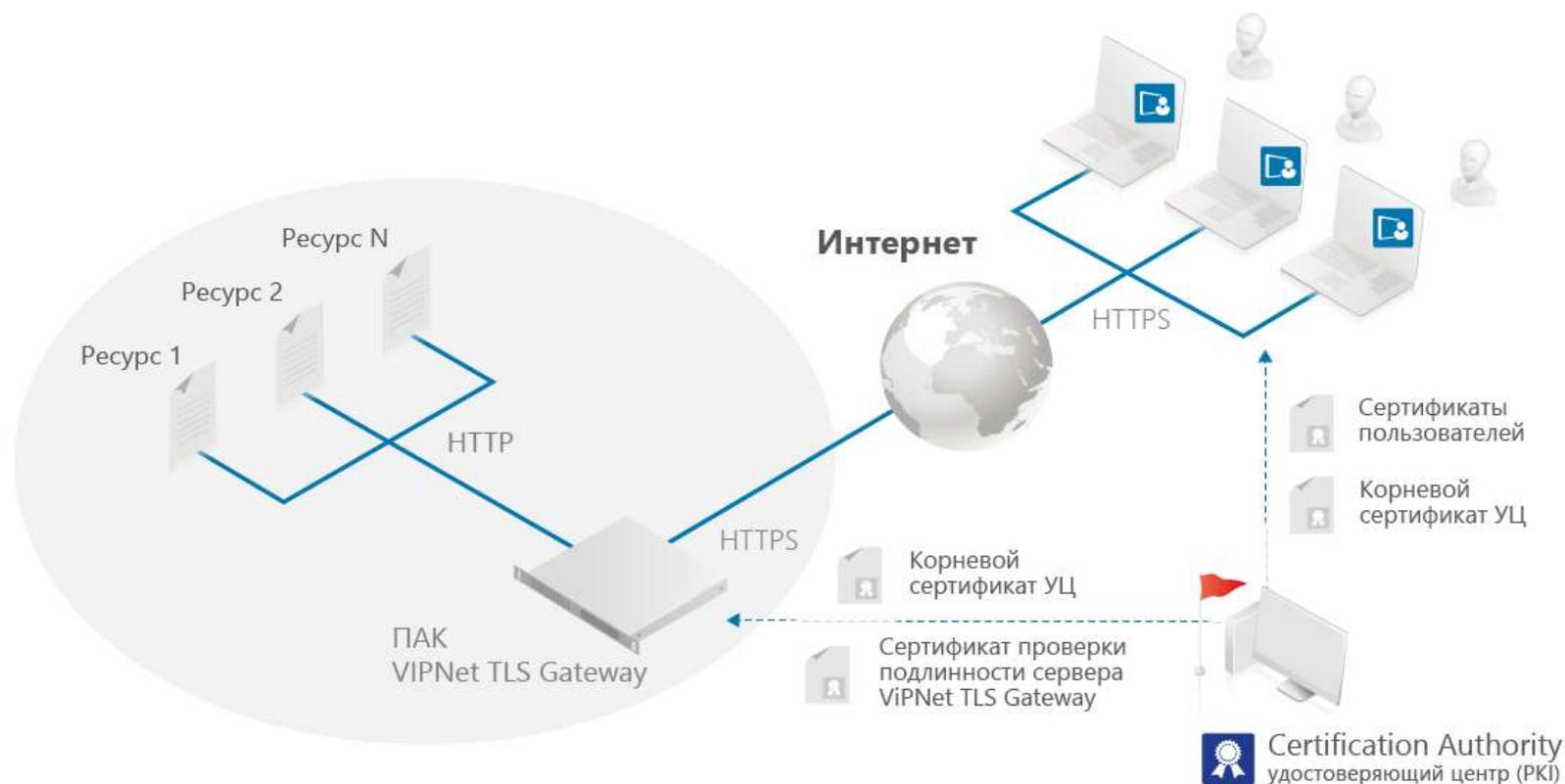
Краткое описание протокола TLS/SSL:

SSL (Secure Sockets Layer) и TLS (Transport Level Security) — криптографические протоколы, обеспечивающие защищенную передачу данных в компьютерной сети. Они широко используются в веб-браузерах, а также при работе с электронной почтой, обмене мгновенными сообщениями и в IP-телефонии.

SSL и TLS представляют собой развитие одной и той же технологии. Аббревиатура TLS появилась в качестве замены обозначения SSL после того, как протокол окончательно стал интернет-стандартом. Такая замена вызвана юридическими аспектами, так как спецификация SSL изначально принадлежала компании Netscape. Во многих случаях названия SSL и TLS продолжают использовать в качестве синонимов, хотя каноническим именем сейчас является TLS. При этом TLS имеет отдельную нумерацию версий и является *более современным* протоколом.



Назначение и основные возможности ViPNet TLS Gateway:



Название исполнения*	TLS 500	TLS 1000	TLS 5000
Пропускная способность в режиме HTTPS-прокси (Мбит/с)	до 250	до 750	до 1000
Количество одновременных соединений	до 4000	до 7000	до 25000
Максимальное число пользователей**	до 3000	до 5000	до 20000

* есть исполнение в виде VA (до 100 клиентов)

** лицензируется отдельно (зависит от требований заказчика). Если используется собственный УЦ, то необходимы лицензии на доп. число сертификатов



Инициализация и настройка ViPNet TLS Gateway:

Подготовка к работе

Развертывание TLS Gateway VA

Активация лицензии

Первичная инициализация

Подготовка рабочего места Администратора и пользователя для
подключения к Web-интерфейсу

Работа с Web-интерфейсом

Подготовка к работе:

- 
- Подготовка сертификатов

- 
- Выделение ip-адресов и портов

- 
- Подготовка лицензии

- 
- Подготовка виртуальной среды и импорт ViPNet TLS Gateway

- 
- Подготовка рабочего места Администратора безопасности

Развертывание TLS VA

Поддерживается работа TLS VA на следующих платформах виртуализации:

- VMware ESXi версии 5 и выше;
- Oracle VM VirtualBox версий 4.3.34 — 5.0.10;
- VMware Workstation версий 8 — 11.

Виртуальная машина, на которой развертывается TLS VA, должна быть сконфигурирована следующим образом:

- количество ядер процессора — не менее 2;
- объем оперативной памяти — не менее 8 Гбайт;
- количество портов Ethernet 10/100/1000 Мбит/с — не менее 3;
- накопители — не менее 50 Гбайт.



Активация лицензии:

```
(C) JSC InfoTeCS, 1991-2017; 1/23 Stary-Petrovsko-Razumovsky passage, building 1, Moscow 127287, Russia
(none) login:
```

```
(C) JSC InfoTeCS, 1991-2017; 1/23 Stary-Petrovsko-Razumovsky passage, building 1, Moscow 127287, Russia
(none) login: root
```

```
Password:
```

```
login[2466]: root login on 'tty1'
```

```
Mode TLS Gateway: Factory settings
```

```
Select network interface for activate license
```

```
0. eth0
```

```
1. eth1
```

```
2. eth2
```

```
3. eth3
```

```
0
```

```
Do you want to use static IP for network interface eth0? (Yes/No)?:
```

```
n
```

```
Do you want to use DNS servers from DHCP? (Yes/No)?:
```

```
y
```

```
Enter full path to license file ( Example: /media/usb0/license.itcslic ):
```

```
/media/usb0/1
```

```
lic_05.09.2017_895707-1.itcslic      lic_30.08.2017_892788-2-TIAS.itcslic  logs.tar.gz
```

```
lic_14.06.2017_844738-1.itcslic      logpr.evtx
```

```
/media/usb0/lic_14.06.2017_844738-1.itcslic
```

```
License has been installed successfully
```

```
Online activation of license...
```

```
License has been activated successfully
```

```
System integrity check started (it will take several seconds)...
```

```
TLS Gateway system version: 1.1.1-474
```

```
System integrity check succeed
```

```
TLS Gateway OS checksum is: D2CD4172
```

```
TLS Gateway software checksum is: 0A5ED3D9
```

```
Do you want to complete the factory settings (Yes/No)?:
```

```
-
```

Первичная инициализация:

```
(C) JSC InfoTeCS, 1991-2017; 1/23 Stary-Petrovsko-Razumovsky
(none) login: root
Password:
login[1417]: root login on 'tty1'
Step "Change root password" was already completed.
Skip (Yes/No)?:
n
Changing password for root.
Enter new password:
11111111
Repeat password:
11111111
Succeed
Do you want to restore a TLS-Gateway backup? (Yes/No)?:
n
Mode TLS Gateway: First initialization
```

Please identify a location so that time zone rules can be set correctly.

Please select a continent or ocean.

- | | | | | | |
|-------------|-----------------|-------------------|--------------|-------------------|---------|
| 1) Africa | 3) Antarctica | 5) Asia | 7) Australia | 9) Indian Ocean | 11) UTC |
| 2) Americas | 4) Arctic Ocean | 6) Atlantic Ocean | 8) Europe | 10) Pacific Ocean | |

#? 8

Please select a country.

- | | | | |
|-------------------------|-------------------|-----------------|------------------|
| 1) Aland Islands | 14) Finland | 27) Lithuania | 40) San Marino |
| 2) Albania | 15) France | 28) Luxembourg | 41) Serbia |
| 3) Andorra | 16) Germany | 29) Macedonia | 42) Slovakia |
| 4) Austria | 17) Gibraltar | 30) Malta | 43) Slovenia |
| 5) Belarus | 18) Greece | 31) Moldova | 44) Spain |
| 6) Belgium | 19) Guernsey | 32) Monaco | 45) Sweden |
| 7) Bosnia & Herzegovina | 20) Hungary | 33) Montenegro | 46) Switzerland |
| 8) Britain (UK) | 21) Ireland | 34) Netherlands | 47) Turkey |
| 9) Bulgaria | 22) Isle of Man | 35) Norway | 48) Ukraine |
| 10) Croatia | 23) Italy | 36) Poland | 49) Vatican City |
| 11) Czech Republic | 24) Jersey | 37) Portugal | |
| 12) Denmark | 25) Latvia | 38) Romania | |
| 13) Estonia | 26) Liechtenstein | 39) Russia | |

#? 39

Please select one of the following time zone regions.

- | | | |
|---------------------------------------|---------------------------------|--|
| 1) MSK-01 - Kaliningrad | 9) MSK+03 - Omsk | 17) MSK+06 - Tomponsky, Ust-Maysky |
| 2) MSK+00 - Moscow area | 10) MSK+03 - Novosibirsk, Tomsk | 18) MSK+07 - Amur River |
| 3) MSK+00 - Crimea | 11) MSK+04 - Altai | 19) MSK+07 - Sakhalin Island |
| 4) MSK+00 - Volgograd, Kirov, Saratov | 12) MSK+04 - Kemerovo | 20) MSK+07 - Oymyakonsky |
| 5) MSK+01 - Astrakhan | 13) MSK+04 - Krasnoyarsk area | 21) MSK+07 - Magadan |
| 6) MSK+01 - Samara, Udmurtia | 14) MSK+05 - Irkutsk, Buryatia | 22) MSK+08 - Sakha (E): North Kuril Is |
| 7) MSK+01 - Ulyanovsk | 15) MSK+05 - Zabaykalsky | 23) MSK+09 - Kamchatka |
| 8) MSK+02 - Urals | 16) MSK+06 - Lena River | 24) MSK+09 - Bering Sea |

#? 2

The following information has been given:

Russia
MSK+00 - Moscow area

Therefore TZ='Europe/Moscow' will be used.

Local time is now: Пнд Окт 23 19:19:22 MSK 2017.

Universal Time is now: Пнд Окт 23 16:19:22 UTC 2017.

Is the above information OK?

Please enter Yes or No

y

Enter a new date(YYYY-MM-DD HH:MM:SS)(Press ENTER if change not required) (current: 2017-10-23 19:19:28):

2017-10-23 16:20:00

Current time: 2017-10-23 16:20:02 MSK

Current time: 2017-10-25 10:40:02 Mon

Initialization of the random number generator...

To generate random 32 bytes press different keys on the keyboard, to interrupt operation input 'cancel'.

Press different keys (0% done)...

Press different keys (1% done)...

Press different keys (2% done)...

Press different keys (3% done)...

Press different keys (4% done)...

Press different keys (5% done)...

Press different keys (6% done)...

Press different keys (7% done)...

Press different keys (8% done)...

Press different keys (13% done)...

Press different keys (12% done)...

Press different keys (11% done)...

Press different keys (10% done)...

Press different keys (9% done)...

Press different keys (8% done)...

Press different keys (22% done)...

Press different keys (33% done)...

Press different keys (43% done)...

Press different keys (52% done)...

Press different keys (60% done)...

Press different keys (68% done)...

Press different keys (69% done)...

Press different keys (70% done)...

Press different keys (77% done)...

Press different keys (78% done)...

Press different keys (85% done)...

Press different keys (86% done)...

Press different keys (92% done)...

Press different keys (93% done)...

Done

sUse GOST R 34.10-2012 256-bit for certificate requests generation? (otherwise GOST R 34.10-2001 will be used) (Yes/No)?:

y

Using GOST R 34.10-2012 256-bit cipher for certificate requests generation

The generation keys process may take several minutes!

Generating keys: 4.9% complete_

```

Type the port for Administration web interface ( Press ENTER to default value use ) ( default: 443 ):
4430
Choose network interface for Administration web interface
0. eth0
1. eth1
2. eth2
3. eth3
0
Type the port for two-way TLS web interface ( Press ENTER to default value use ) ( default: 443 ):
4431
Choose network interface for two-way TLS web interface
0. eth0
1. eth1
2. eth2
3. eth3
0
Type the port for one-way TLS web interface ( Press ENTER to default value use ) ( default: 443 ):
4432
Choose network interface for one-way TLS web interface
0. eth0
1. eth1
2. eth2
3. eth3
0
Select network interface for access to proxied resources
0. eth0
1. eth1
2. eth2
3. eth3
0
Enter settings for network interface eth0 which will be used for: "Administration web interface", "Two-way TLS web interface",
One-way TLS web interface", "Access to proxied resources"
Enter IP address:
192.168.1.1
Enter netmask ( Press ENTER to use default value ) ( default: 255.255.255.0 ):
255.255.255.0
Enter a default gateway:
192.168.1.2
Enter a new DNS servers (Press ENTER if change not required) (use ';' for separation)( current: 127.0.0.1 ):
8.8.8.8
Selected DNS servers: 8.8.8.8
Do you want to select a new DNS servers (Yes/No)?:
n

```

```

Enter folder to create requests for transport certificates ( Example: /media/usb0/ ):
/media/usb0/
12/
12.p10
123.txt
3597/
LocaleMetaData/
MR/
MR2/
SMART_ID.CRD
System Volume Information/
URLы плагинов.txt
ViPNet PKI Client Почта России/
ViPNet_CSP_RUS_4.2.8.46116_BETTA.exe
ViPNet_PKI_Client_TLS_Unit_Admin's_Guide_ru.pdf
abn_0001.dst
admin.pfx
admin.nginx.req
/media/usb0/MR
certcrl.crl
certnew (1).cer
certnew (2).cer
lic_05.09.2017_095707-1.itcslic
lic_14.06.2017_844738-1.itcslic
lic_30.08.2017_892788-2-TIAS.itcslic
logpr.evtx
logs.tar.gz
root_certificate.cer
root_certificate.pem
tias_root.crt
tls (002).zip
tls root.cer
tls_oneside_nginx.req
tls_twoside_nginx.req
Комплект пользователя/
File /media/usb0/MR/admin_nginx.req has been saved
File /media/usb0/MR/tls_oneside_nginx.req has been saved
File /media/usb0/MR/tls_twoside_nginx.req has been saved

```

Request certificates has been created successfully

```

Enter full path for CA root certificate ( Example: /media/usb0/root_certificate.pem ):
/media/usb0/12
12/ 12.p10 123.txt
/media/usb0/12/
admin.cer ca.cer req/ sos.crl
/media/usb0/12/ca.cer
Enter full path to CRL ( Example: /media/usb0/certcrl.crl ):
/media/usb0/12/sos.crl
Do you want to install other CA certificate or/and CRL? (Yes/No)?
n

```

```

Enter folder where placed transport certificates ( Example: /media/usb0/ ):
/media/usb0/12/
Founded transport certificate /media/usb0/12/1.cer
Founded transport certificate /media/usb0/12/2.cer
Founded transport certificate /media/usb0/12/3.cer

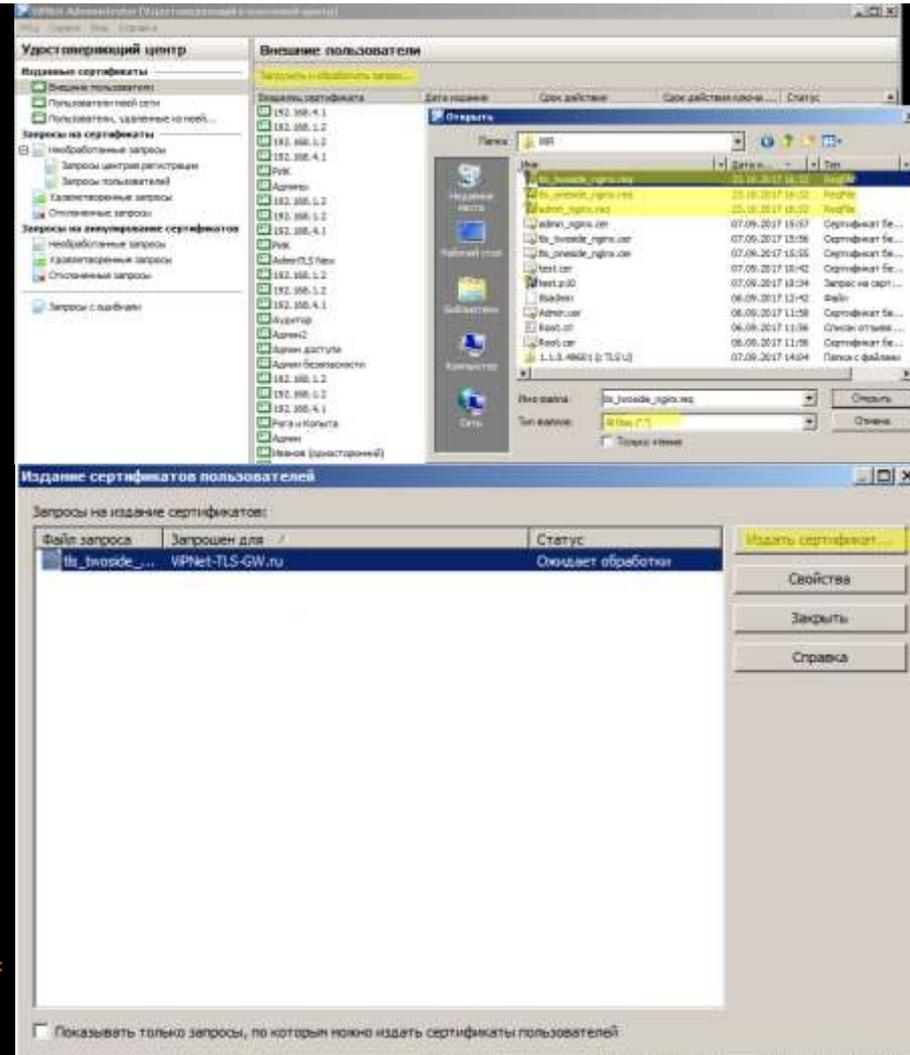
```

Transport certificates are installed successfully

```

Enter full path for Security administrator certificate ( Example: /media/usb0/ivanov.crt ):
/media/usb0/12/admin.cer
Security administrator was created successfully
Generating system configuration, please wait...

```



The screenshot shows the Windows Certificate Management console. The left pane displays the 'Certificates' tree with 'Issued Certificates' expanded. The right pane shows a list of issued certificates for the user 'Ivanov'. A dialog box titled 'Имя сертификата' is open, showing a list of certificates. The 'twoside_nginx.req' certificate is selected. Below the dialog, a table shows the status of the request.

Файл запроса	Запрошен для	Статус
twoside_nginx.req	WPNet-TLS-GW.ru	Ожидает обработки

Buttons: Издать сертификат..., Свойства, Закрыть, Справка.

Checkbox: Показывать только запросы, по которым можно издать сертификаты пользователей

Подготовка рабочего места Администратора и пользователя для подключения к Web-интерфейсу:

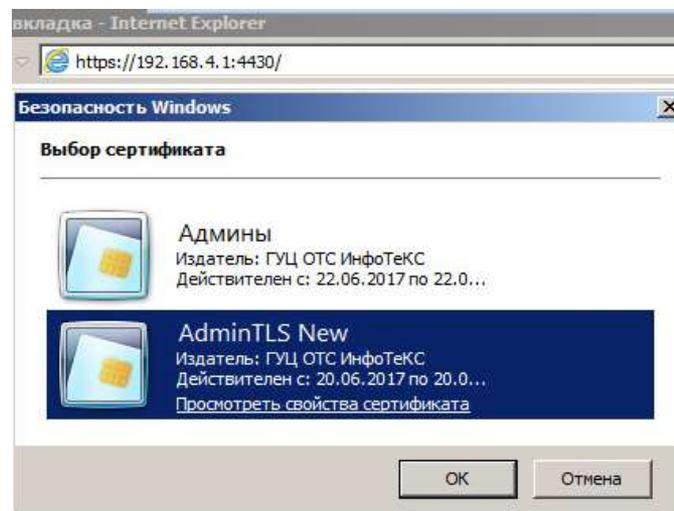
Для того чтобы начать работу с механизмами электронной подписи, выполните следующие действия:

- Установите контейнер ключей:
- Если закрытый ключ и сертификат находятся в одном контейнере, и этот контейнер размещен в папке на диске, см. раздел Установка контейнера ключей из папки.
- Если закрытый ключ и сертификат находятся в одном контейнере и размещены на внешнем устройстве, см. раздел Установка контейнера ключей с внешнего устройства.
- Если сертификат был издан в удостоверяющем центре по запросу, и в результате имеется контейнер ключей и отдельный файл сертификата, см. раздел Установка сертификата в контейнер ключей.
- Установите сертификат в системное хранилище.
- Установите сертификаты издателей и список аннулированных сертификатов (CRL) в системное хранилище.



Для подключения к веб-интерфейсу по протоколу TLS выполните следующие действия:

- Откройте веб-браузер Internet Explorer и в адресной строке введите `https://<адрес сетевого интерфейса администрирования ViPNet TLS Gateway:порт>`.
- В появившемся окне со списком сертификатов выберите свой сертификат, который вы установили в системное хранилище ОС Windows



После успешной двусторонней аутентификации будет установлено защищенное соединение по протоколу TLS. Откроется страница веб-интерфейса ViPNet TLS Gateway, где будут доступны действия в соответствии с вашей ролью.

Работа с Web-интерфейсом:

1 - Меню «Сертификаты удостоверяющих центров»

2 - Поиск сертификатов

3 - Кнопка «Импортировать...»

4 - Кнопка «Скачать сертификат»

5 - Кнопка «Проверить наличие обновлений CRL каждые: 0 часов»

6 - Кнопка «Обновить»

7 - Кнопка «Состояние системы»

8 - Кнопка «Настройка»

CRYPOT2-CA

Владелец	Организация	Статус сертификата	Статус CRL
CRYPOT2-CA		Действителен	Действителен

Сведения

СЕРТИФИКАТ

Владелец: CRYPOT2-CA

Организация:

Серийный номер: 726D41DDEB4E33A742A6A35EBB96F25

Кем выдан: CRYPOT2-CA

Статус сертификата: Действителен

Срок действия сертификата: с 07.07.2016 по 07.07.2017

Скачать сертификат

CRL

Проверить наличие обновлений CRL каждые: 0 часов

07:06:08 - 09.03.2017

Сертификаты адми...

- Поиск сертификатов
- Владелец
 - AdminTLS New
 - Админы

Редактирование полномочий администратора

СЕРТИФИКАТ

Владелец:	AdminTLS New
Организация:	
СНИЛС:	
Серийный номер:	01D2E9CBFD5CB5700000000C1ACC0001
Кем выдан:	ГУЦ ОТС ИнфоТеКС
Статус сертификата:	Действителен
Срок действия сертификата:	с 20.06.2017 по 20.06.2018

полномочия администратора

- Администратор безопасности**
Управляет списком доверенных УЦ, транспортными ключами VIPNet TLS Gateway и полномочиями учетных записей, имеющих доступ к административному интерфейсу
- Администратор доступа**
Управляет доступом пользователей к ресурсам и списком веб-ресурсов
- Аудитор**
Отвечает за просмотр и архивацию журнала аудита

AdminTLS New

полномочия администратора

Администратор безопасности
Управляет списком доверенных УЦ, транспортными ключами VIPNet TLS Gateway и полномочиями учетных записей, имеющих доступ к административному интерфейсу

Администратор доступа
Управляет доступом пользователей к ресурсам и списком веб-ресурсов

Аудитор
Отвечает за просмотр и архивацию журнала аудита

СЕРТИФИКАТ

Владелец:	AdminTLS New
Организация:	
СНИЛС:	
Серийный номер:	01D2E9CBFD5CB5700000000C1ACC0001
Кем выдан:	ГУЦ ОТС ИнфоТеКС
Статус сертификата:	Действителен
Срок действия сертификата:	с 20.06.2017 по 20.06.2018

Ссылка на сертификат

Ресурсы

Поиск ресурсов ...   

Наименование	Адрес ресурса	Суффикс подключения
<input type="checkbox"/> www-web	192.168.4.4:81	https://192.168.1.2:8080/web
<input type="checkbox"/> 667	sch667u.mskobr.ru:80	https://192.168.1.2:8080/667
<input type="checkbox"/> SSTU	ccty.ru:443	https://192.168.1.2:8088/stu

www-web

Адрес ресурса: http://192.168.4.4:81

Адрес подключения пользователей: https://192.168.1.2:8080/web

Порт VIPNet TLS Gateway для подключения к ресурсу: 40000

Тип аутентификации по TLS- протоколу: Двусторонняя

Запросов на предоставление доступа: 0

Зарегистрировано пользователей: 2

Новый защищаемый ресурс

Шаг 1: Укажите общую информацию о ресурсе.

Наименование:

Логотип: 

Описание:

Новый защищаемый ресурс

Шаг 2: Настройте параметры подключения к ресурсу

Адрес ресурса: // :

Адрес, по которому к ресурсу обращается VIPNet TLS Gateway

Внешние подключения пользователей

Тип аутентификации: Односторонняя Двусторонняя

Суффикс:

Указанный суффикс добавляется к внешним адресам VIPNet TLS Gateway (см. Настройки сети), которые используются для подключения пользователей с указанным типом аутентификации, и образуют адрес подключения

Использовать выделенный порт

Адреса подключения: https://192.168.1.2:8080/

VIPNet TLS Gateway Admin TLS New ▾

УПРАВЛЕНИЕ

- Мониторинг
- Запросы на предоставление доступа
- Сертификаты пользователей
- Разрешенные**
- Блокированные
- Сертификаты администраторов
- Веб-ресурсы

Сертификаты пользователей, которым разрешено подключение по TLS-протоколу

Поиск сертификатов ...

<input type="checkbox"/>	Владелец	Организация	СНИЛС	Статус сертификата
<input type="checkbox"/>	РИК			Действителен
<input type="checkbox"/>	РИК	РИК		Действителен
<input type="checkbox"/>	РИК			Действителен

Добавление сертификатов пользователей

Шаг 2: Проверка списка загруженных сертификатов

Владелец	СНИЛС	Статус сертификата
<input checked="" type="checkbox"/> РИК		Новый

Назад Далее Закрыть

Добавление сертификатов пользователей

Шаг 3: Назначение прав доступа к ресурсам

Поиск ресурсов ...

www-web	Доступен	Блокировать
667 счмпвапвапва	Разрешить	Блокировать

Назад Сохранить Закрыть

Типовые вопросы и ошибки при настройке ViPNet TLS Gateway:



A sunset scene with a warm, orange and yellow sky. In the foreground, several wind turbines are silhouetted against the bright light. In the background, a series of high-voltage power lines stretch across the horizon. The sun is low on the right side, partially obscured by clouds.

**Спасибо!
Вопросы...**