ИНСТРУКЦИЯ ПО УСТАНОВКЕ ЦИФРОВОГО СЕРТИФИКАТА БЕЗОПАСНОСТИ

Аннотация

Инструкция для Клиентов компании АО “ASTEL” пользующихся услугой «Фильтрация и анализ трафика»

Оглавление

1. Для чего это нужно?

Сегодня все современные Web-сервисы успешно перешли на использование защищенного ***HTTPS-протокола.***

Пользуясь услугой Бизнес Интернет, с включенной функцией SSL Inspection, Клиент тем самым дает свое согласие на вскрытие зашифрованного трафика на программно-аппаратных комплексах компании ASTEL, для обеспечения возможности морфологического анализа контента, проведения антивирусной проверки, применения политик Web Filter и осуществления фильтрации на основе протоколов – Application Filter.

Чтобы это стало возможно с технической точки зрения, весь клиентский трафик, Оператор пропускает через специализированные устройства, которые могут в режиме реального времени осуществлять все эти необходимые операции.

Однако, современные браузеры, беспокоясь о пользователе, будут всегда выводить предупреждения системы безопасности, если сертификат осуществляющий подпись сертификата «на лету» запрошенного пользователем сайта, будет отсутствовать в системном хранилище сертификатов в качестве доверенного.

Именно для этих целей необходимо установить сертификат системы DPI который является само подписанным сертификатом Центра Сертификации (Certificate Authority)

Таблица 1. Данные о сертификате (действителен до 01 февраля 2019г)

Серийный номер: 00 bc 0a 76 a0 19 01 53 09

Алгоритм подписи: sha256RSA

Алгоритм хэширования подписи: sha256

Срок действия: с 21 апреля 2017 по 16 апреля 2037

Алгоритм отпечатка: sha1

Отпечаток: 6f b8 03 a2 73 c4 a4 5d ad e4 0c 62 d4 30 32 b4 6f 07 c0 b3

Таблица 2. Данные о сертификате (действителен с 01 февраля 2019г)

Серийный номер: 00 fe 9c 4d 1f 43 ee b1 3b

Алгоритм подписи: sha256RSA

Алгоритм хэширования подписи: sha256

Срок действия: с 6 декабря 2018 по 1 декабря 2039

Алгоритм отпечатка: sha1

Отпечаток: c9 d3 5c 7d f0 db b3 fd 4a d1 21 38 8e 32 5c cb 85 0c ed 40

2. Установка сертификата.

После скачивания файла сертификата с официального сайта компании ASTEL, на локальную машину, необходимо провести процедуру его установки в хранилище доверенных сертификатов.

Эта процедура отличается для различных операционных систем:

- Установка под операционную систему Windows Vista/7/10
- Установка под операционную систему Linux
- Установка под операционную систему MAC OS

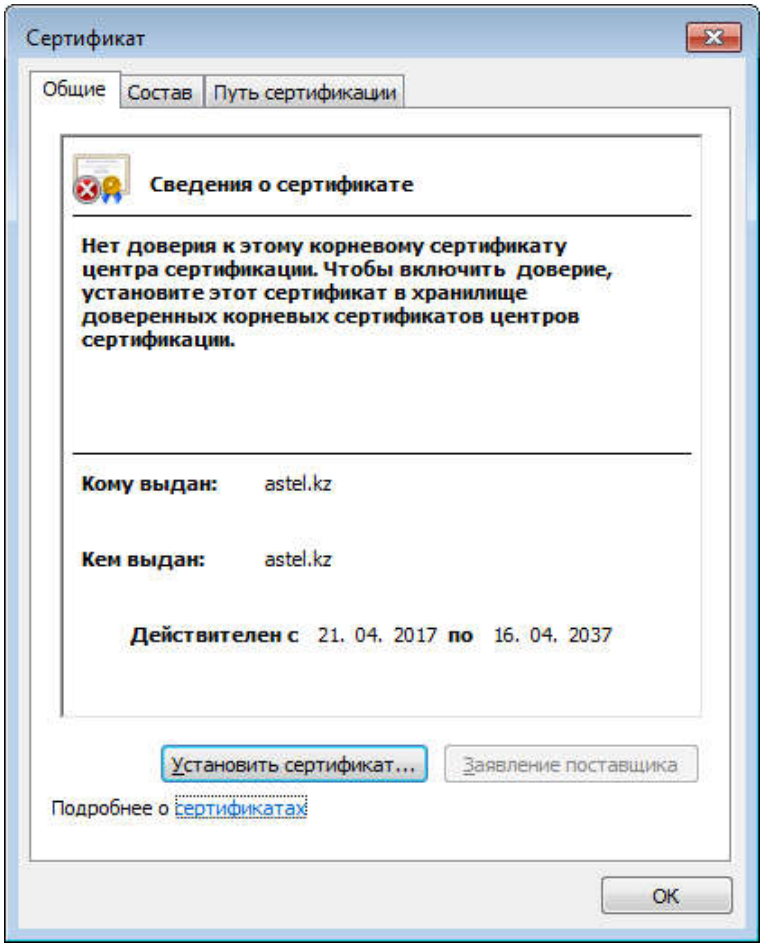
a. Установка сертификата под операционную систему Windows Vista/7/10.

i. Командная строка.

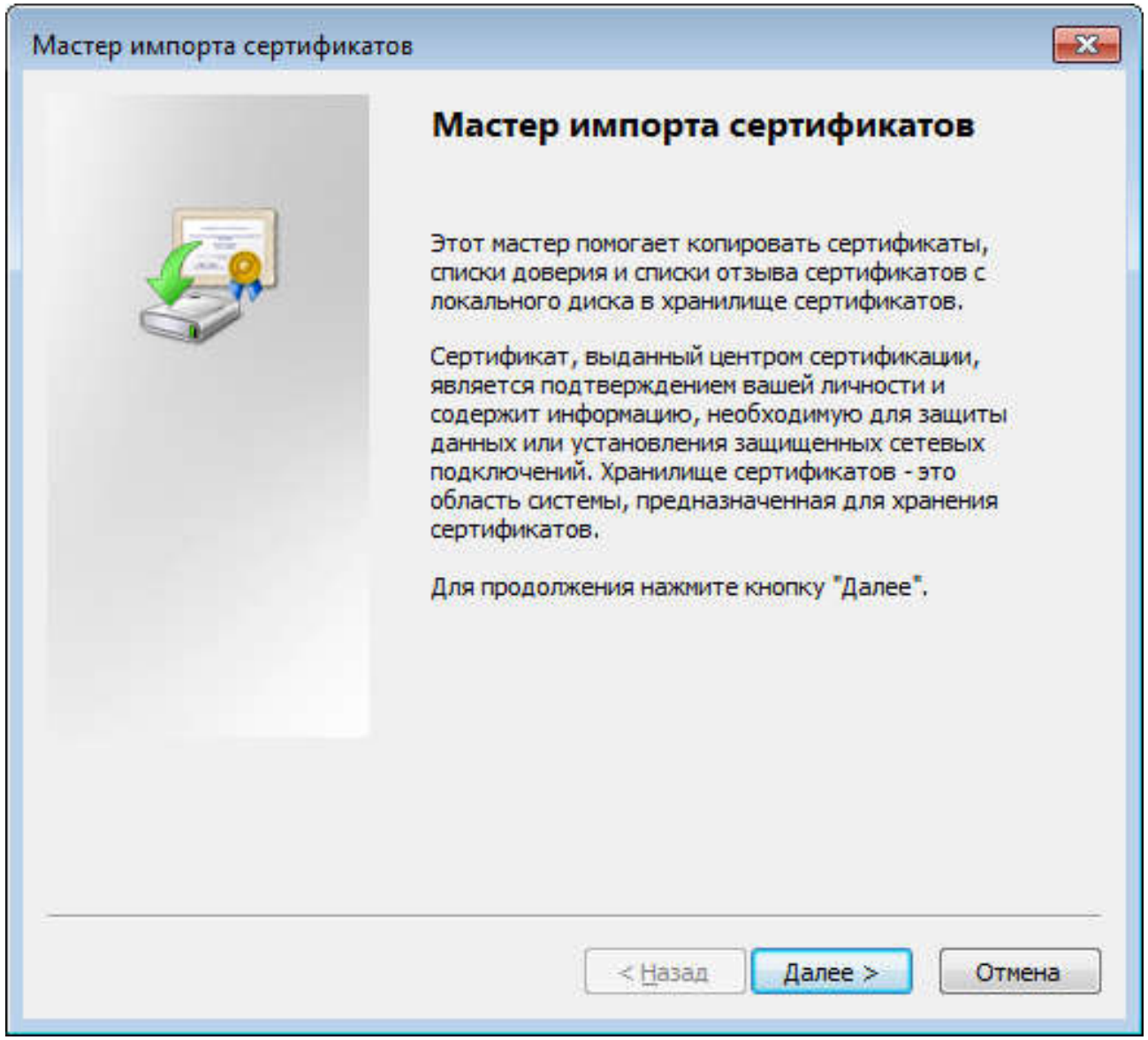
Функция	Метод
Добавить	Скопируйте файл на диск X, используйте команду: certutil -addstore -f "ROOT" X:\ASTEL-FG-SSL.cer где X – идентификатор диска.
Удалить	Используйте команду: certutil -delstore "ROOT" serial-number-hex

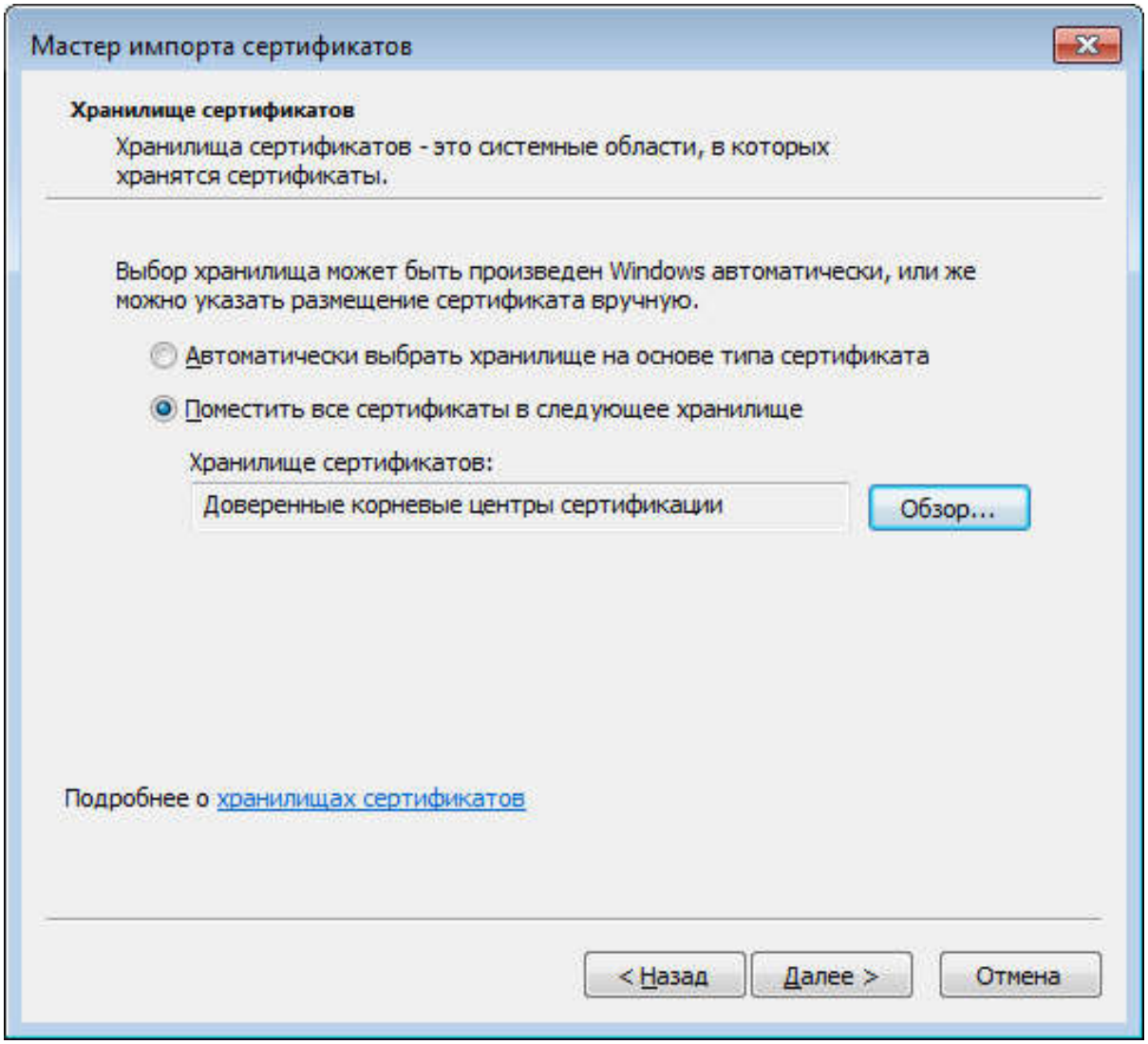
ii. С использованием графического интерфейса.

Открываем файл сертификата. Операционная система предупреждает пользователя, что данный сертификат является не доверенным.

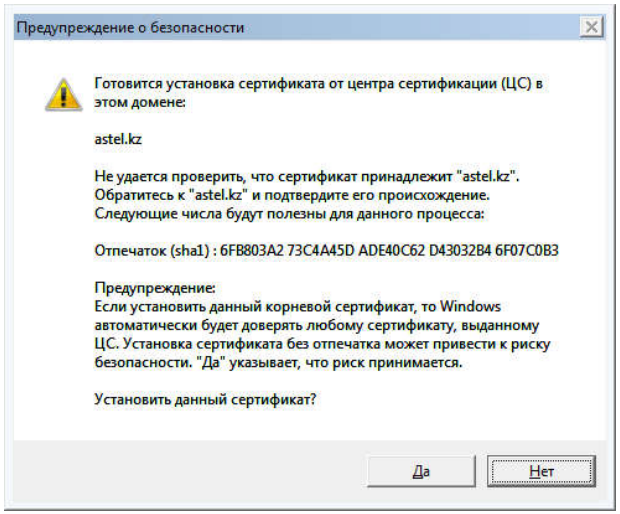


Нажимаем «Установить сертификат». Запустится мастер установки сертификатов.


Мастер импорта сертификатов
Мастер импорта сертификатов
Этот мастер помогает копировать сертификаты, списки доверия и списки отзыва сертификатов с локального диска в хранилище сертификатов.
Сертификат, выданный центром сертификации, является подтверждением вашей личности и содержит информацию, необходимую для защиты данных или установления защищенных сетевых подключений. Хранилище сертификатов - это область системы, предназначенная для хранения сертификатов.
Для продолжения нажмите кнопку "Далее".
< Назад
Далее >
Отмена

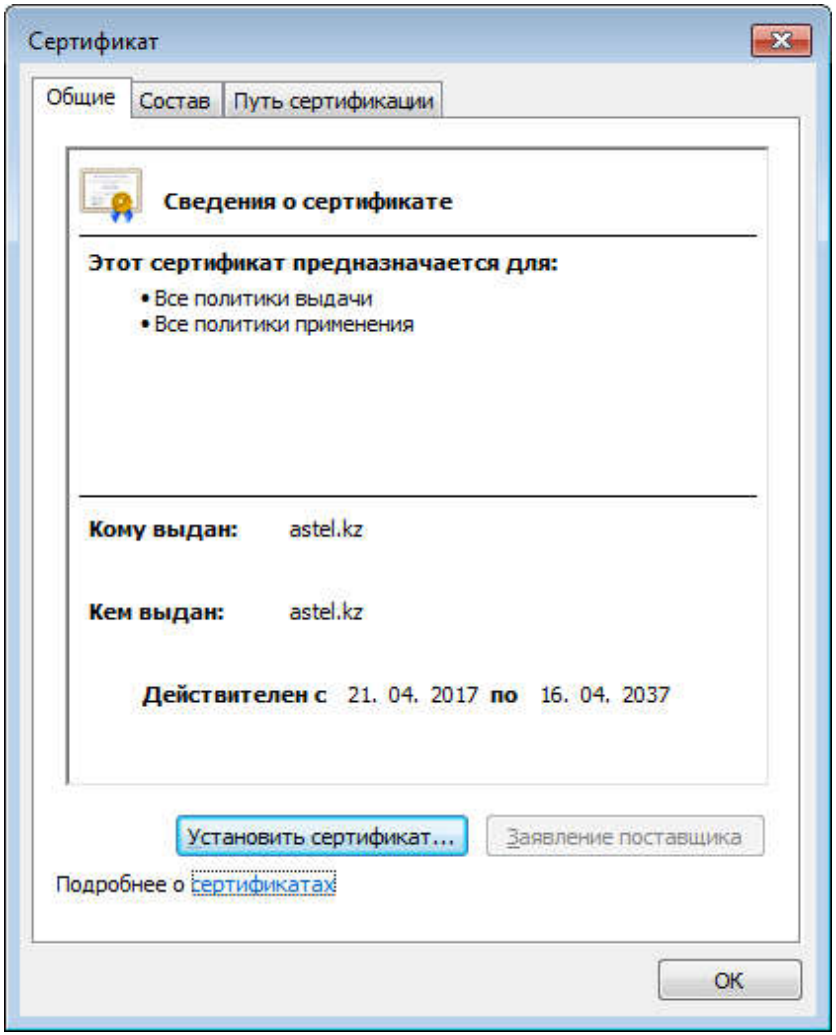


Выбираем контейнер «Доверенные корневые центры сертификации» и нажимаем Далее.



Нажимаем «Да».

После этого, если мы еще раз попробуем открыть сертификат, никаких предупреждающих надписей, об отсутствии доверия, мы увидеть не должны.



Важно!!!

Браузеры Google Chrome и Microsoft IE используют общий системный контейнер сертификатов. Однако Mozilla Firefox использует свой собственный репозиторий сертификатов. Если вашим основным браузером является Firefox, процедура установки для него описана ниже.

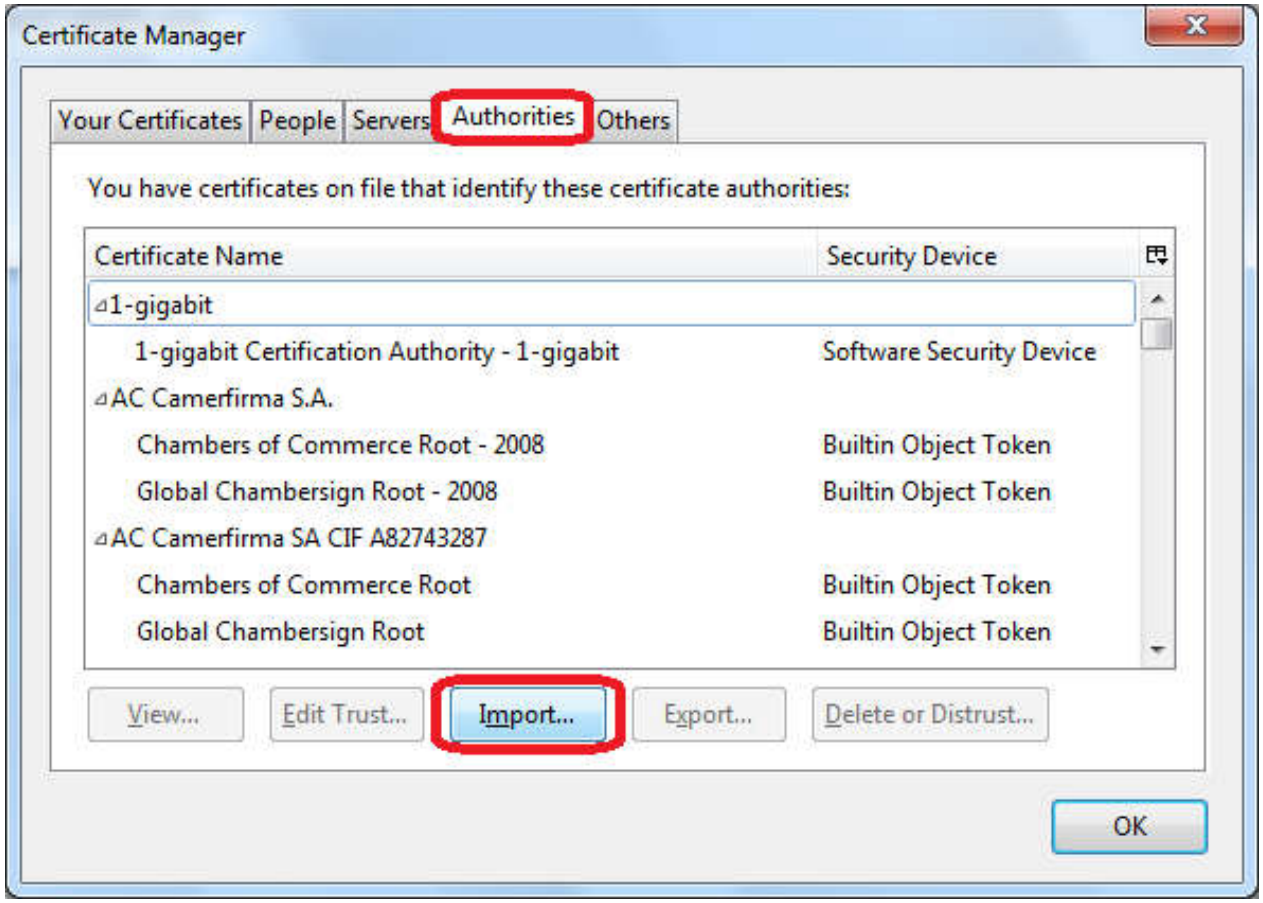
Opera браузер использовал свое собственное корневое хранилище сертификатов, но с осени 2013 года она больше не делает этого.

В более новых версиях Opera (14 и более поздних) используется корневое хранилище, предоставляемое операционной системой. В более старых версиях Opera (версии с 9.5 по 12) используется встроенное хранилище Opera.

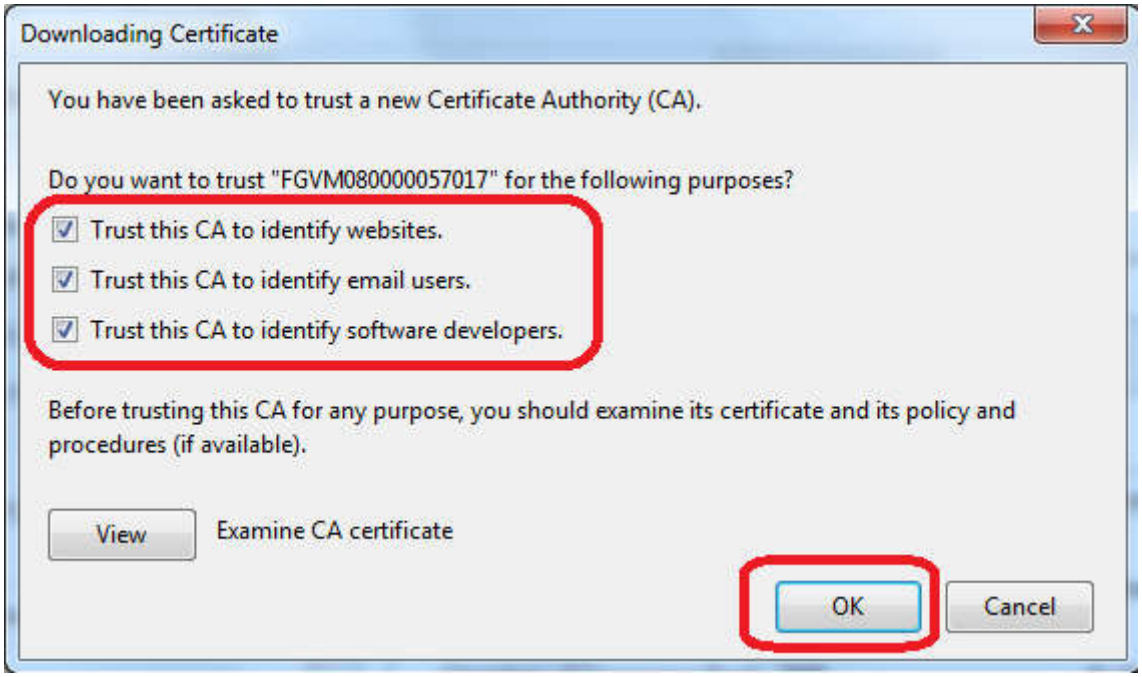
Для установки сертификата в Firefox:

Переходим в Menu > Options > Advanced > Certificates > View Certificates:

Переходим на вкладку «Authorities» > Import.

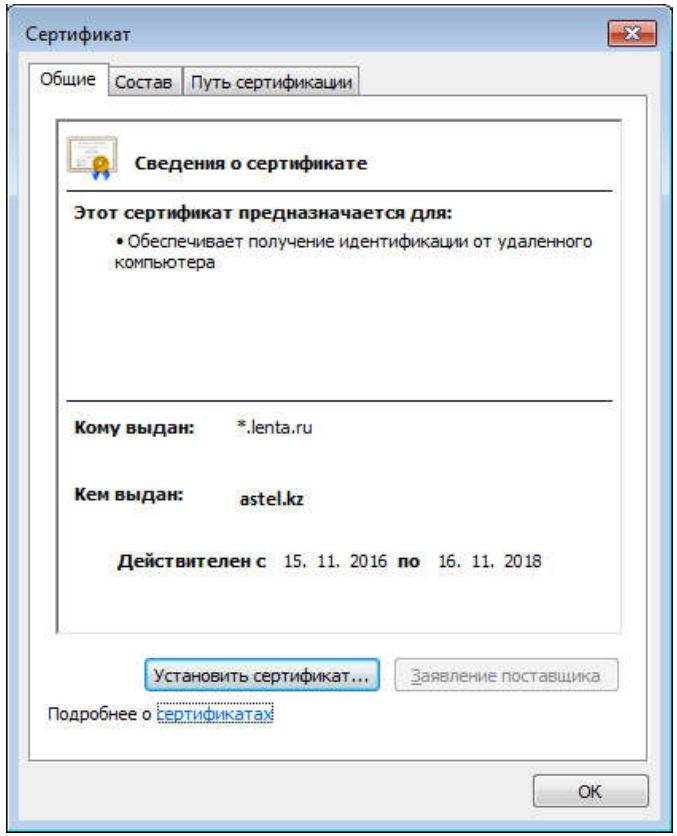

Certificate Manager
Your Certificates
People
Servers
Authorities
Others
You have certificates on file that identify these certificate authorities:
Certificate Name
Security Device
1-gigabit
1-gigabit Certification Authority - 1-gigabit
Software Security Device
AC Camerfirma S.A.
Chambers of Commerce Root - 2008
Builtin Object Token
Global Chambersign Root - 2008
Builtin Object Token
AC Camerfirma SA CIF A82743287
Chambers of Commerce Root
Builtin Object Token
Global Chambersign Root
Builtin Object Token
View...
Edit Trust...
Import...
Export...
Delete or Distrust...
OK

Далее:



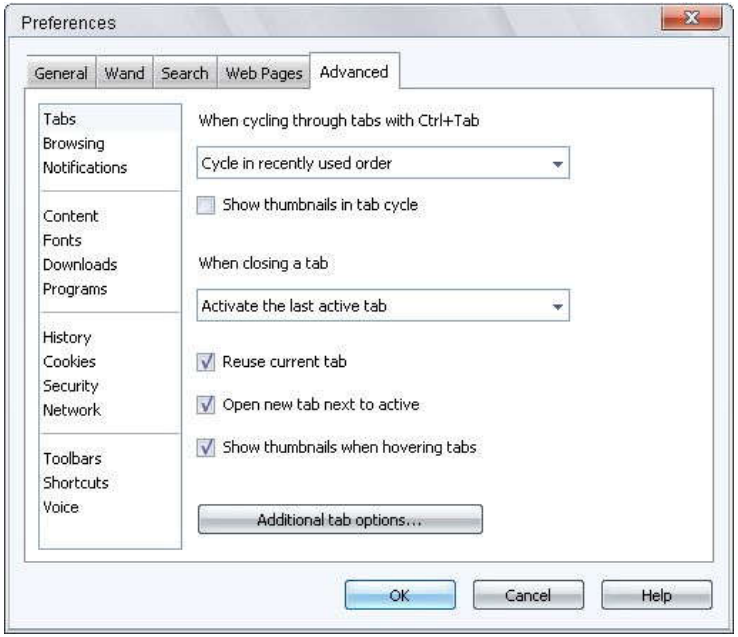
Проверяем доступ перейдя на любой URL с использованием протокола HTTPS. Убедиться, что сертификат установлен правильно можно перейдя на любой ресурс с использованием HTTPS, например https://lenta.ru

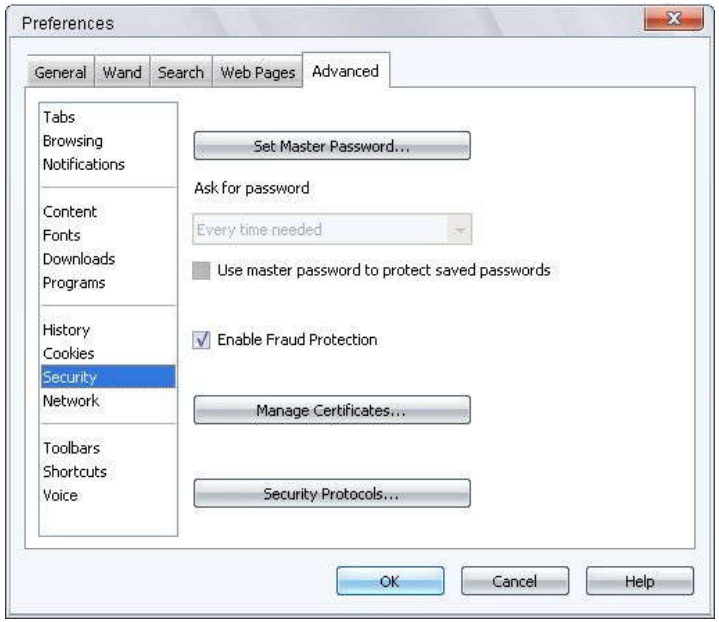
Поле «Кем выдан» должно содержать “astel.kz”.



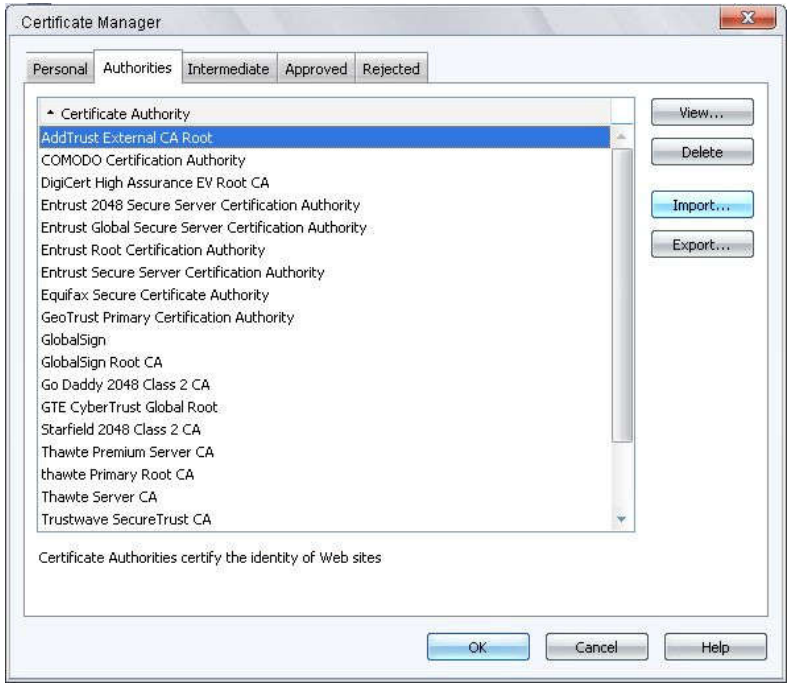
Для установки сертификата в старых версиях Opera (до 14 версии):

Переходим в Tools> Preferences> Advanced> Security> Manage Certificates:

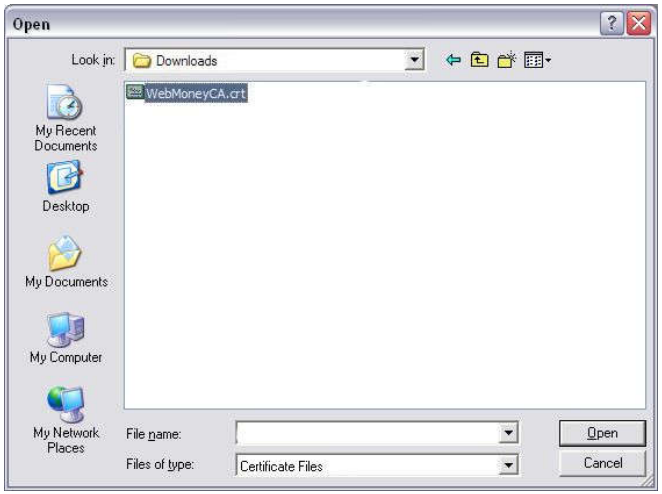

Preferences
General
Wand
Search
Web Pages
Advanced
Tabs
Browsing
Notifications
Content
Fonts
Downloads
Programs
History
Cookies
Security
Network
Toolbars
Shortcuts
Voice
When cycling through tabs with Ctrl+Tab
Cycle in recently used order
Show thumbnails in tab cycle
When closing a tab
Activate the last active tab
Reuse current tab
Open new tab next to active
Show thumbnails when hovering tabs
Additional tab options...
OK
Cancel
Help


Preferences
General
Wand
Search
Web Pages
Advanced
Tabs
Browsing
Notifications
Content
Fonts
Downloads
Programs
History
Cookies
Security
Network
Toolbars
Shortcuts
Voice
Set Master Password...
Ask for password
Every time needed
Use master password to protect saved passwords
Enable Fraud Protection
Manage Certificates...
Security Protocols...
OK
Cancel
Help

Кликаем на кнопку «Manage Certificates» > Import.

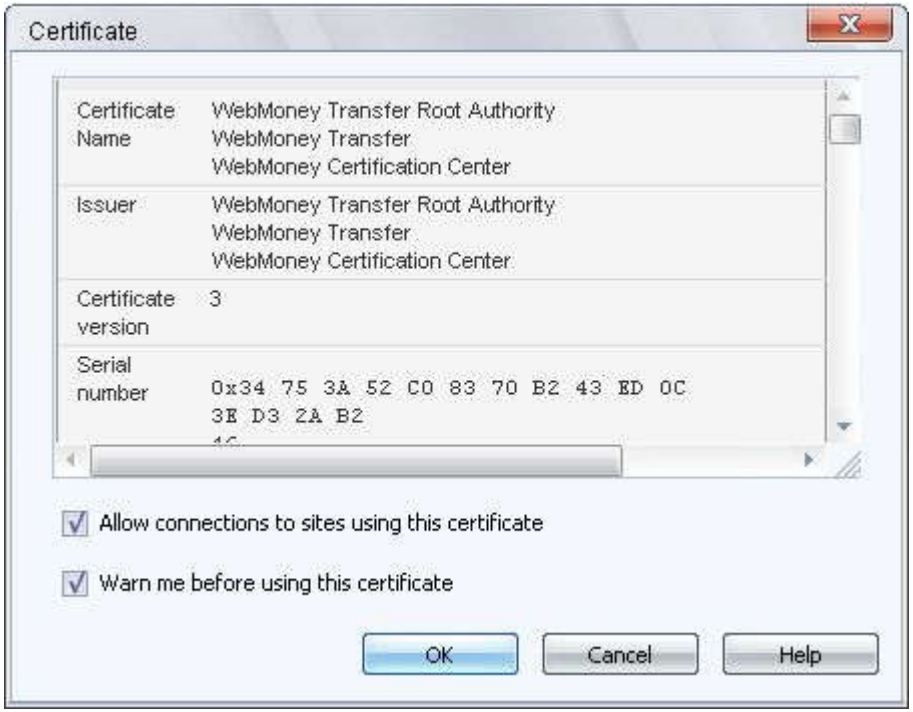


Выберите сохраненный сертификат на локальном диске и нажмите кнопку «Открыть» / «Open».



Перед тем как инсталлировать сертификат щелкните кнопку «View», чтобы проверить валидность сертификата, посмотреть его серийный номер и отпечаток.

Также мы крайне рекомендуем снять галочку с параметра «*Warn me before using this certificate*»!!!



Данный скриншот дан только для иллюстрации, и не соответствует серийным номерам сертификатам компании ASTEL!

Внимание!!!

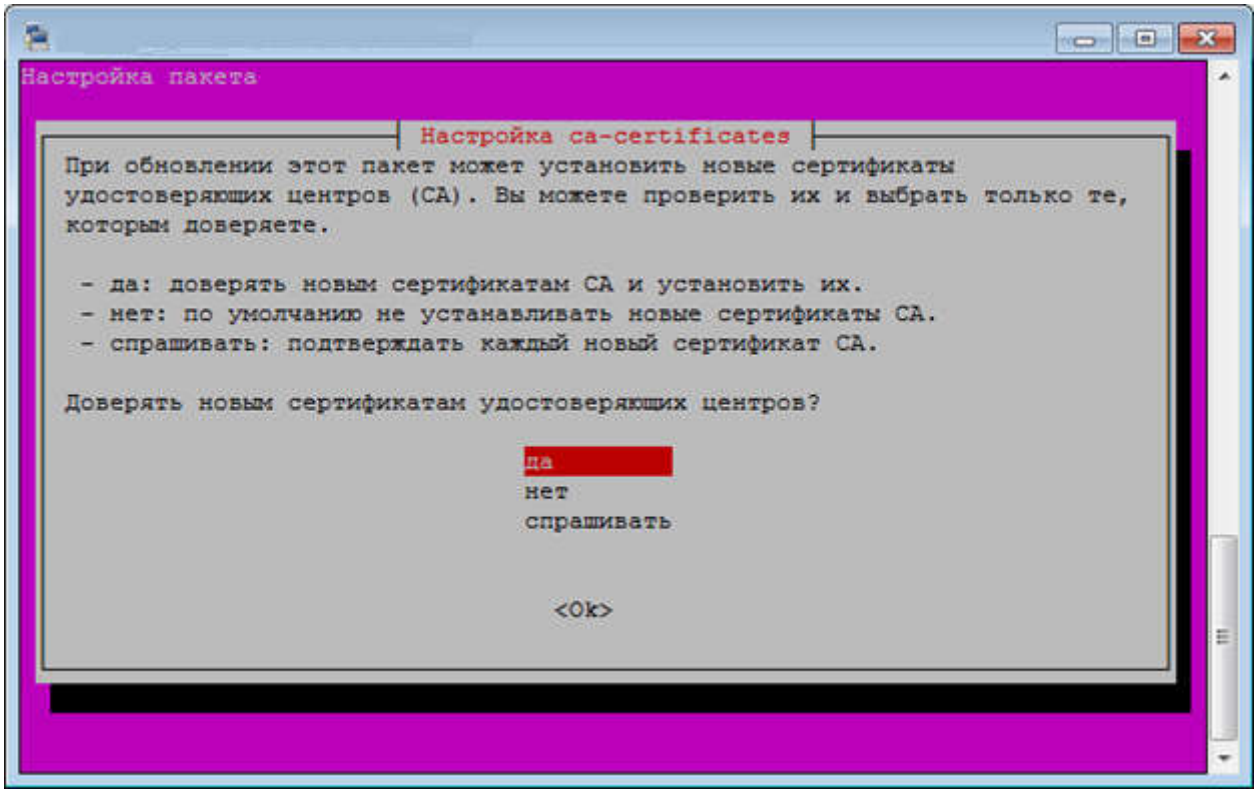
Компания ASTEL, заботится о безопасности своих Клиентов и сохранности их конфиденциальной информации, поэтому ресурсы, попадающие в категории **“Healts and Welness”**, **“Finance and Banking”**, если не указано иное в Протоколе политики безопасности, не будут подвергнуты SSL инспектированию, при условии, что они разрешены к просмотру!!!

Если есть необходимость закрыть данные категории, SSL инспекция данных категорий будет включена!!!

Узнать к какой категории относится тот иной ресурс в сети Интернет, в базе данных Fortigate, Клиенты могут проверить по данному адресу:

b. Установка сертификата на ОС LINUX (Mint/Ubuntu/Debian).

Функция	Метод
Добавить	Копируем файл на локальную машину. Для того чтобы добавить корневые сертификаты необходимо выполнить 3 простых шага. Создаем каталог для CA сертификатов **/usr/share/ca-certificates** sudo mkdir /usr/share/ca-certificates/extra Копируем 'ASTEL-FG-SSL.cer' файл в созданный ранее каталог sudo cp ASTEL-FG-SSL.crt /usr/share/ca-certificates/extra/ ASTEL-FG-SSL.crt Переконфигурируем пакет ca-certificates sudo dpkg-reconfigure ca-certificates



Выделяем нужные сертификаты, в данном случае ASTEL-FG-SSL.crt и жмем OK.

c. Установка сертификата на ОС LINUX (CentOs 5)

Функция	Метод
Добавить	Добавьте ваш доверенный сертификат в файл /etc/pki/tls/certs/ca-bundle.crt cat ASTEL-FG-SSL.crt >>/etc/pki/tls/certs/ca-bundle.crt

d. Установка сертификата на ОС LINUX (CentOs 6)

Функция	Метод
Добавить	1. Установите ca-certificates package: yum install ca-certificates 2. Включите функцию динамической конфигурации CA: update-ca-trust force-enable 3. Добавьте ваш файл в директорию /etc/pki/ca-trust/source/anchors/: cp ASTEL-FG-SSL.crt /etc/pki/ca-trust/source/anchors/ 4. Запустите команду: update-ca-trust extract

e. Установка сертификата под MAC OS

Функция	Метод
Добавить	Используйте команду: sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain ~/ASTEL-FG-SSL.crt
Удалить	Используйте команду: sudo security delete-certificate -c "<name of existing certificate>"