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?	.2
Таб.	лица 1. Данные о сертификате	.3
2.	Установка сертификата	.3
a.	Установка сертификата под операционную систему Windows Vista/7/10	.4
i.	Командная строка	.4
ii.	С использованием графического интерфейса	.4
b.	Установка сертификата на OC LINUX (Mint/Ubuntu/Debian)	18
c.	Установка сертификата на OC LINUX (CentOs 5)	19
d.	Установка сертификата на OC LINUX (CentOs 6)	20
e.	Установка сертификата под MAC OS	20

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: c 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: c 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

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

і. 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

іі. С использованием графического интерфейса.

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

Сертификат	×
Общие Состав Путь сертификации	
🙀 Сведения о сертификате	
Нет доверия к этому корневому сертификату центра сертификации. Чтобы включить доверие, установите этот сертификат в хранилище доверенных корневых сертификатов центров сертификации.	
Кому выдан: astel.kz	
Кем выдан: astel.kz	
Действителен с 21. 04. 2017 по 16. 04. 2037	
I Установить сертификат Заявление поставщик Подробнее о сертификатах	a
0	ĸ

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 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

Мастер импорта сертификатов
Хранилище сертификатов
Хранилища сертификатов - это системные области, в которых хранятся сертификаты.
Выбор хранилища может быть произведен Windows автоматически, или же можно указать размещение сертификата вручную.
💿 Автоматически выбрать хранилище на основе типа сертификата
Оместить все сертификаты в следующее хранилище
Хранилище сертификатов:
Доверенные корневые центры сертификации Обзор
Подробнее о <u>хранилищах сертификатов</u>
< <u>Н</u> азад Далее > Отмена

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

Предупреждение о безопасности

Готовится установка сертификата от центра сертификации (ЦС) в этом домене:

astel.kz

Не удается проверить, что сертификат принадлежит "astel.kz". Обратитесь к "astel.kz" и подтвердите его происхождение. Следующие числа будут полезны для данного процесса:

Отпечаток (sha1): 6FB803A2 73C4A45D ADE40C62 D43032B4 6F07C0B3

Предупреждение:

Если установить данный корневой сертификат, то Windows автоматически будет доверять любому сертификату, выданному ЦС. Установка сертификата без отпечатка может привести к риску безопасности. "Да" указывает, что риск принимается.

Установить данный сертификат?



Нажимаем «Да».

X

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

- 6	Сведени	я о сертификате	
Этс	т сертифик • Все полити • Все полити	ат предназначае іки выдачи іки применения	тся для:
Kon	у выдан:	astel.kz	
Keø	выдан: Действите	astel.kz елен с 21.04.201	7 no 16. 04, 2037
	Устано	вить сертификат	Заявление поставщик

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.

Орега 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.

You have certificates on file that identify these certificat	e 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 Exp.	ort Delete or Distrust	

Далее:

Downloading Certificate
You have been asked to trust a new Certificate Authority (CA).
Do you want to trust "FGVM080000057017" for the following purposes?
Trust this CA to identify websites.
Trust this CA to identify email users.
Trust this CA to identify software developers.
Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).
View Examine CA certificate
OK Cancel

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".

бщие	Состав Путь сертификации
Это	 Сведения о сертификате т сертификат предназначается для: Обеспечивает получение идентификации от удаленного компьютера
Ком	у выдан: *.lenta.ru
Кем	выдан: astel.kz Действителен с 15, 11, 2016 по 16, 11, 2018
Тодроб	Установить сертификат Заявление поставщика нее о сертификатах

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

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

General	Wand	Search	Web Pages	Advanced			
Tabs		W	hen cycling thi	rough tabs with Ctrl+Tab			
Browsin Notifica	wsing ifications		/cle in recently	y used order 🛛 👻			
Content Fonts Downloads Programs			Show thumbnails in tab cycle				
		w	hen closing a t	tab			
		A	Activate the last active tab				
History Cookies Security Networl	: / k	V	Reuse currer Open new ta	nt tab ab next to active			
Toolbar Shortcu	s Its	V	Show thumb	nails when hovering tabs			
voice			Addition	nal tab options			

General	Wand	Search	Web Pages	Advanced			
Tabs Browsing Notifications			Set Ma	ster Password			
Content Fonts Downloads Programs		As Ev	Ask for password Every time needed Use master password to protect saved passwords				
History Cookies Security	History Cookies		Enable Frauc	d Protection			
Networ	k		Manag	e Certificates			
Toolbar Shortcu Voice	s ts		Secur	ity Protocols			

Кликаем на кнопку «Manage Certificates» > Import.

+ Contril	ficato Authori	hu .				View
AddTrue	External CA					-
COMOD	O Certification	n Authority			<u></u>	Delete
DigiCert	High Accuran	re FV Poot CA				
Entrust 2	2048 Secure 1	Server Certifical	ion Authorit	v		Import
Entrust	Global Secure	Server Certific	ation Author	, itv		importeri
Entrust I	Root Certifica	tion Authority		55 6 7 7		Export
Entrust	Secure Serve	r Certification A	uthority			
Equifax	Secure Certifi	icate Authority	12			
GeoTrus	t Primary Cer	tification Author	ity			
GlobalSig	յո					
GlobalSig	gn Root CA					
Go Dadd	ly 2048 Class	2 CA				
GTE Cyb	erTrust Globa	al Root				
Starfield	2048 Class 2	CA				
Thawte	Premium Serv	er CA			1	
thawte P	Primary Root	CA				
Thawte :	Server CA					
Trustwa	ve SecureTru	ist CA			*	
Contificat	te Authoritica	cartify the idee	titu of Wat	citoc		2
Cerdificat	le Authondes	cercity the iden	icity of web	SILES		

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»!!!

<localhost></localhost>			
Certificate authoriti only install certificat	es certify the iden e authorities from	tity of Web sites. sites you trust.	You should
WebMoney Transfe	r Root Authority		View

Certificate Name	WebMoney Transfer Root Authority WebMoney Transfer WebMoney Certification Center	E
Issuer	WebMoney Transfer Root Authority WebMoney Transfer WebMoney Certification Center	
Certificate version	×3	
Serial number	0x34 75 3& 52 CO 83 70 B2 43 MD 0C 3M D3 ZA B2	
€ [
√ Allow coni √ Warn me	nections to sites using this certificate before using this certificate	

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



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 OC 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 СА 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 ОК.

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

е. Установка сертификата под МАС ОЅ

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 certificate="" existing="" of="">"</name>