# Сертификаты

Модуль «Сертификаты» расположен в Меню «Защита». Данный модуль предназначен для управления сертификатами, которые используются для установления защищённых SSL/TLS соединений типа клиент-сервер. Более подробно о SSL/TLS можно почитать здесь https://ru.wikipedia.org/wiki/SSL и https://ru.wikipedia.org/wiki/TLS.

Созданные сертификаты могут применяться как в «ИКС», так и в сторонних программах.

При первой установке «ИКС» автоматически создаются конечные сертификаты для WEBинтерфейса, телефонии и почты.

<b>Добавить</b> Удал	ить Просмотр сертификата	🛓 Импорт	🛓 Экспорт 👻				<b>Q</b> Поиск
Название 🔺		Тип сертиф	фиката	Закрытый ключ	Создан	Действует до	Имя или адрес хоста
🗆 🌞 Сертификаты							
Autogenerate	ed Asterisk_5db98833462f26.531858	31 Конечный с	сертификат	не зашифрован	30.10.2019	30.10.2029	ics-asterisk
Autogenerate	ed GUI_5db988310e40a5.57388659	Конечный с	сертификат	не зашифрован	30.10.2019	30.10.2029	ics-gui
Autogenerate	ed MailServer_5db988315ad5a2.1653	3086 Конечный с	сертификат	не зашифрован	30.10.2019	30.10.2029	ics-mail-server

Список сертификатов представлен в виде дерева, а поле модуля поделено на столбцы, в которых показана основная информация о сертификатах: тип ключа родительского сертификата, дата начала действия и окончания, а также имя хоста (или ip-адрес), который представляет данный сертификат.

Модуль позволяет создать новый сертификат или удалить существующий при помощи кнопок «Создать» и «Удалить»; экспортировать созданные сертификаты или импортировать сторонние при помощи кнопок «Экспорт» и «Импорт»; просматривать информацию о выбранном сертификате при помощи кнопки «Просмотр сертификата».

# Создание сертификатов

Чтобы создать новый сертификат, нажмите «Добавить».

#### Добавление сертификата

Общее	Настройки	Использование ключа	Netscape расширение		
Название <sup>*</sup>					
Новый сер	отификат				
Код страны					
RU - Russia	an Federation		-		
Город		(	Область		
Организация		E	-mail		
Имя или адре	с хоста *				
test.ru					
			Добавить Отмена		

Во вкладке «Общее» заполняются данные сертификата: наименование, код страны, местоположение, сведения об организации, имя хоста или ip-адрес.

#### Добавление сертификата

	•
Тип шифрования	
▼ RSA	
	Тип шифрования • RSA

Во вкладке «Настройки» определяется роль сертификата - СА (корневой) или конечный, устанавливается метод шифрования, время действия и длина ключа в битах.

Добавление сертификата				
Общее	Настройки	Использование ключа	Netscape расширение	
Шаблон				
CA				•
Использовани	еключа			
CRL sign				
<ul> <li>Certificat</li> </ul>	e Sign			
Non Repu	udiation			
Digital Sig	gnature			
Key Encip	herment			
Расши <mark>ренное</mark>	использование кл	юча		
E-mail Pro	otection			
TLS Web	Client Authentical	tion		
Code Sign	ning			
TLS Web	Server Authentica	tion		
Time Star	nping			
			Лобавить	Отмена

Во вкладке «Использование ключа» можно выбрать шаблон использования открытого ключа сертификата в поле «Шаблон» или указать вручную в разделах «Использование ключа» («Key usage extensions») и «Расширенное использование ключа» («Extended key usage»). Более подробно можно почитать здесь

https://www.ibm.com/support/knowledgecenter/en/SSKTMJ\_9.0.1/admin/conf\_keyusageextensionsand extendedkeyusage\_r.html

Общее Настройн	и Использование ключа	Netscape расширение	
SSL Client			
SSL Server			
S/MIME			
Object Signing			
SSL CA			
S/MIME CA			
Object Signing CA			

Во вкладке «Netscape расширение» можно указать использование ключа для совместимости со старыми Netscape приложениями (выпущенными до принятия стандарта X.509 v3).

После нажатия кнопки «Добавить» будет предложено зашифровать ключ паролем. Введите пароль или откажитесь от его использования.

🔘 Шифровать закрытый ключ паролем		
<ul> <li>Не шифровать закрытый ключ</li> </ul>		
	Ок	Отмена

Важно: для служб ИКС всегда применяются только нешифрованные сертификаты.

Важно: первоначально всегда должен создаваться корневой сертификат, затем дочерние конечные сертификаты! К службам ИКС(кроме SSL-фильтрации), применяются только конечные сертификаты. Будьте внимательны: неверное применение сертификата к службам может сделать их недоступными для пользователя!

### Удаление сертификатов

Документация - https://doc-old.a-real.ru/

Для удаления сертификата выделите нужный сертификат в списке (или несколько сертификатов зажав клавишу Ctrl) и нажмите кнопку «Удалить»:

Вы действители	ьно хотите удалить эти элементы?
Новый сертификат Сертификат	
Новый сертификат2 Сертификат	
	Ок Отмена

Если сертификат используется какой-либо службой «ИКС», то будет выдано уведомление об ошибке:



### Импорт/экспорт сертификатов

Для импорта сертификата нажмите кнопку «Импорт»:

Импорт	
Сертификат *	Ключ сертификата
*	*
Пароль сертификата в формате РКСS 12	
	Ок Отмена
	Ок Отмена

В полях «Сертификат» и «Ключ сертификата» выбираются файл сертификата и файл ключа соответственно. Для импорта сертификата в формате PKCS12 необходимо в поле «Сертификат» выбрать соответствующий файл и в поле «Пароль сертификата в формате PKCS 12» указать пароль.

Для экспорта сертификата нажмите кнопку «Экспорт» и выберите необходимый вариант:



## Просмотр сертификата

Для просмотра выделите нужный сертификат в списке и нажмите кнопку «Просмотр сертификата»:

Общее		
Название:	Autogenerated GUI_5cece744c3edb1.30259507	
Код страны:	RU - Russian Federation	
Имя или адрес хоста:	ics-gui	
Настройки		
Тип сертификата:	Конечный сертификат	
Алгоритм:	SHA 256	
Тип шифрования:	RSA	
Создан:	28.05.2019	
Действует до:	29.05.2029	
Длина ключа:	2048 бит	
Использование ключа		
Использование ключа:	Digital Signature Key Encipherment	
Расширенное использование ключа:	TLS Web Server Authentication	

From: https://doc-old.a-real.ru/ - **Документация** 

Permanent link: https://doc-old.a-real.ru/doku.php?id=ics70:serts&rev=1573402802

Last update: 2020/01/27 16:28

