Сертификаты

Общие положения

SSL (Secure Sockets Layer — уровень защищённых сокетов) — криптографический протокол, который обеспечивает установление безопасного соединения между клиентом и сервером. Протокол обеспечивает конфиденциальность обмена данными между клиентом и сервером, использующими TCP/IP, причём для шифрования используется асимметричный алгоритм с открытым ключом. При шифровании с открытым ключом используется два ключа, причем любой из них может использоваться для шифрования сообщения. Тем самым, если используется один ключ для шифрования, то соответственно для расшифровки нужно использовать другой ключ. В такой ситуации можно получать защищённые сообщения, публикуя открытый ключ, и храня в тайне секретный ключ. Для работы SSL требуется, чтобы на сервере имелся SSL-сертификат.

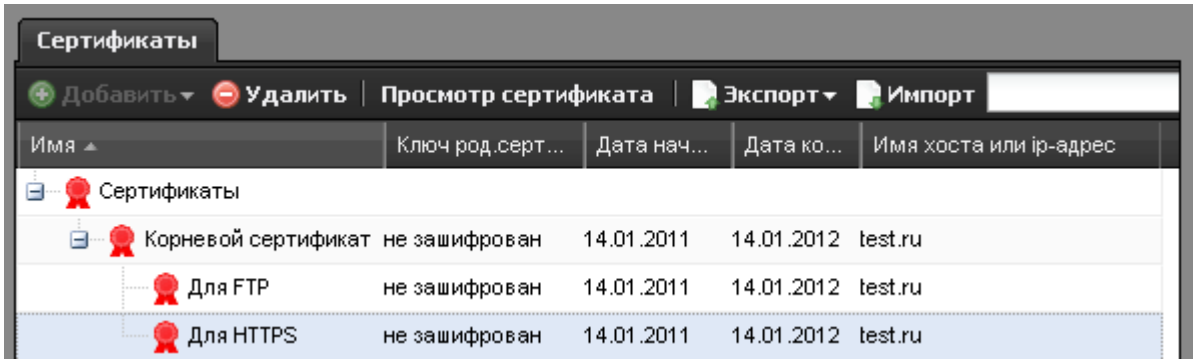
Цифровой сертификат — выпущенный удостоверяющим центром электронный или печатный документ, подтверждающий принадлежность владельцу открытого ключа или каких-либо атрибутов.

Реализация происходит следующим образом:

1. Клиент инициирует соединение,
2. В ответ сервер посылает цифровой идентификатор (сертификат). Если требуется аутентификация клиента, то сервер может запросить ответный сертификат,
3. Клиент сверяет идентификатор сервера, при необходимости отправляя свой,
4. После завершения процесса аутентификации клиент передает серверу ключ сессии, зашифрованный при помощи открытого ключа сервера,
5. На основе сгенерированного ключа устанавливается защищенное соединение и

происходит передача данных между клиентом и сервером;

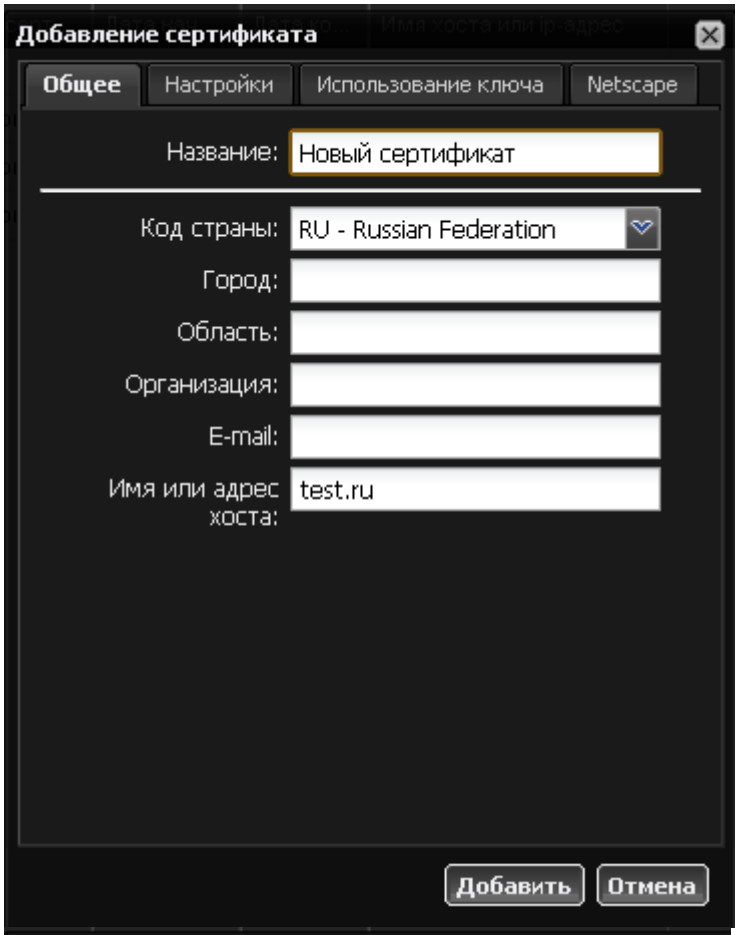
В разделе «Сертификаты» хранится список всех SSL-сертификатов, применяющихся в службах ИКС.

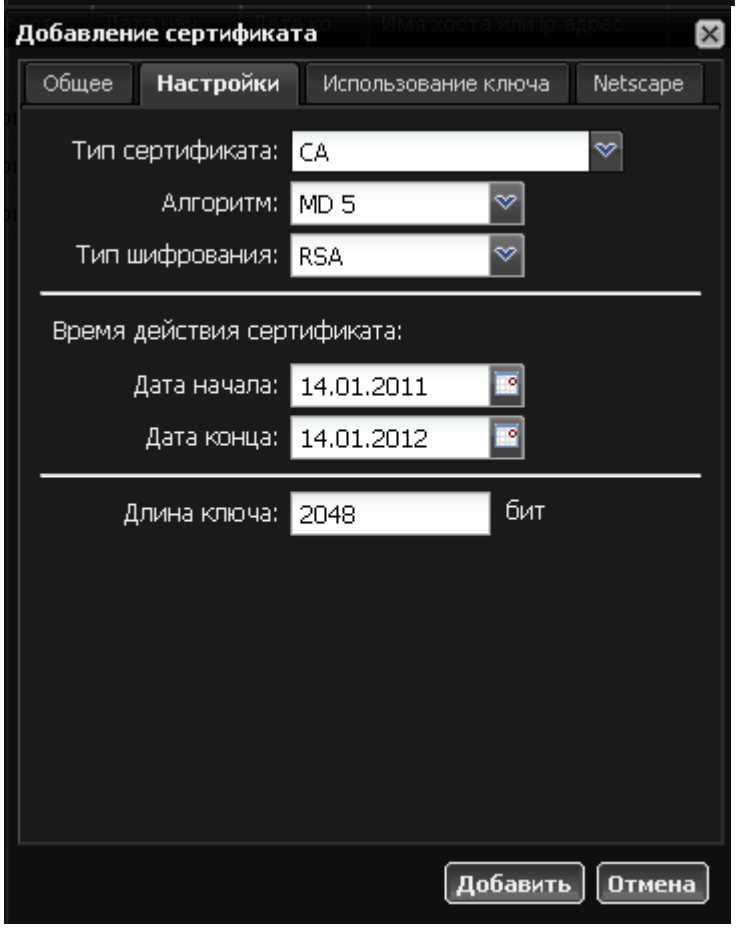


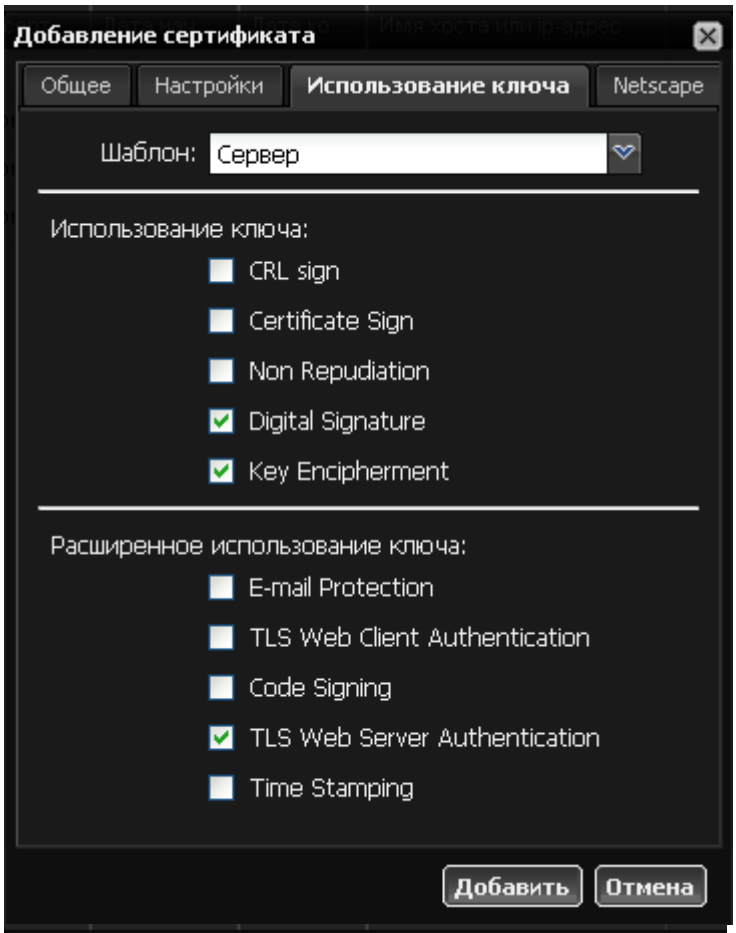
Как обычно, список сертификатов представлен в виде дерева, а поле модуля поделено на столбцы, в которых показана основная информация о сертификатах: тип ключа родительского сертификата, дата начала действия и окончания, а также имя хоста (или ip-адрес), который представляет данный сертификат. Вы также можете экспортировать созданные сертификаты или импортировать сторонние при помощи кнопок «Экспорт» и «Импорт», а также просматривать информацию о выбранном сертификате при помощи кнопки «Просмотр сертификата».

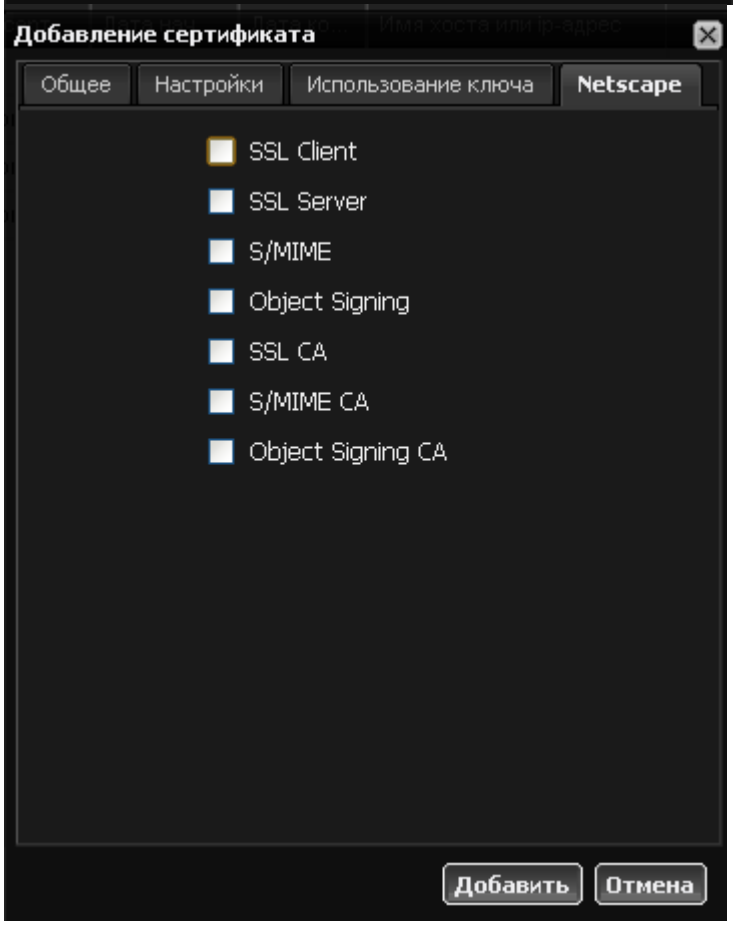
Создание сертификатов

Чтобы создать новый SSL-сертификат, нажмите «Добавить» → «Сертификат».


Добавление сертификата
Общее
Настройки
Использование ключа
Netscape
Название:
Новый сертификат
Код страны:
RU - Russian Federation
Город:
Область:
Организация:
E-mail:
Имя или адрес хоста:
test.ru
Добавить
Отмена


Добавление сертификата
Общее
Настройки
Использование ключа
Netscape
Тип сертификата:
CA
Алгоритм:
MD 5
Тип шифрования:
RSA
Время действия сертификата:
Дата начала:
14.01.2011
Дата конца:
14.01.2012
Длина ключа:
2048
бит
Добавить
Отмена



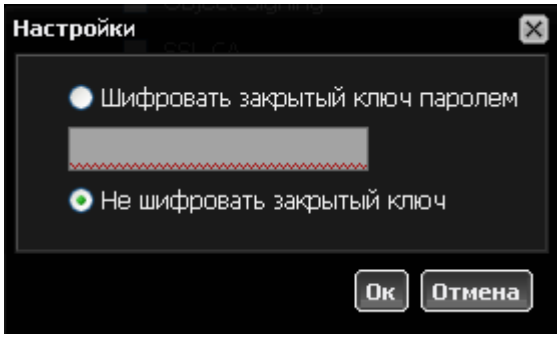


Сначала заполняются данные сертификата - наименование, код страны, местоположение, сведения об организации, имя хоста или ip-адрес. Затем во вкладке «Настройки» определяется

роль сертификата - CA (корневой) или конечный, устанавливается метод шифрования, время действия и длина ключа в битах.

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!

После этого перейдите во вкладку «Использование ключа» и выберите в списке необходимый шаблон использования. Выбор шаблона автоматически установит флажки параметров сертификата применительно к выбранной роли. Если вы опытный системный администратор, вы можете установить флажки вручную. Вкладка «Netscape» позволяет установить дополнительные netscape-расширения для сертификата.



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

Важно: для служб ИКС всегда применяются только нешифрованные сертификаты.