


# Особенности эксплуатации СА на роутерах Mikrotik: резервное копирование, экспорт и импорт сертификатов

 [interface31.ru/tech\\_it/2021/07/osobennosti-ekspluatacii-ca-na-routerah-mikrotik-rezervnoe-kopirovanie-eksport-i-import-sertifikatov.html](https://interface31.ru/tech_it/2021/07/osobennosti-ekspluatacii-ca-na-routerah-mikrotik-rezervnoe-kopirovanie-eksport-i-import-sertifikatov.html)

Mikrotik предоставляет пользователям достаточно широкие возможности, одна из них - создание на роутере собственного **центра сертификации (CA)**, который позволяет управлять собственной **инфраструктурой открытых ключей (PKI)**.

Благодаря этому вы можете выпускать, подписывать и отзываться сертификаты, а также поддерживать доверительные отношения без использования дополнительных технических и программных средств. Это удобно, но эксплуатация СА на базе Mikrotik имеет свои особенности и подводные камни, которые нужно четко представлять и учитывать при выборе такого решения.



## Онлайн-курс по MikroTik

Научиться настраивать MikroTik с нуля или систематизировать уже имеющиеся знания можно на [углубленном курсе по администрированию MikroTik](#). Автор курса, сертифицированный тренер MikroTik Дмитрий Скоромнов, лично проверяет лабораторные работы и контролирует прогресс каждого своего студента. В три раза больше информации, чем в вендорской программе MTCNA, более 20 часов практики и доступ навсегда.

Коротко напомним, что такое **инфраструктура открытых ключей (PKI)**, это область доверия, где каждый участник может доверять другому участнику, не имея никаких предварительных данных о нем. В основе PKI лежит **центр сертификации (CA)**, авторитет СА неоспорим, а доверие к нему не подвергается сомнению.

При создании СА генерируется ключевая пара из **закрытого ключа** и **корневого сертификата**, который содержит открытый ключ. Закрытый ключ является секретным и должен храниться как зеница ока, потому как его компрометация дает возможность злоумышленнику выпускать сертификаты от имени вашего СА, а следовательно, получить доступ к вашей области доверия. Корневой сертификат, наоборот, должен быть широко распространен на узлах вашей области доверия, так как именно он позволяет убедиться в подлинности выпущенных сертификатов.

При этом любой пользователь или узел, располагающий корневым сертификатом, может в любой момент времени убедиться в подлинности предъявленного ему сертификата другого пользователя или узла, а так как доверие к СА не подвергается сомнению, то автоматически возникают доверительные отношения с

предъявителем действующего сертификата. Также корневой сертификат содержит адрес **CRL** - списка отозванных сертификатов, что позволяет дополнительно убедиться, что предъявленный сертификат не был отозван.

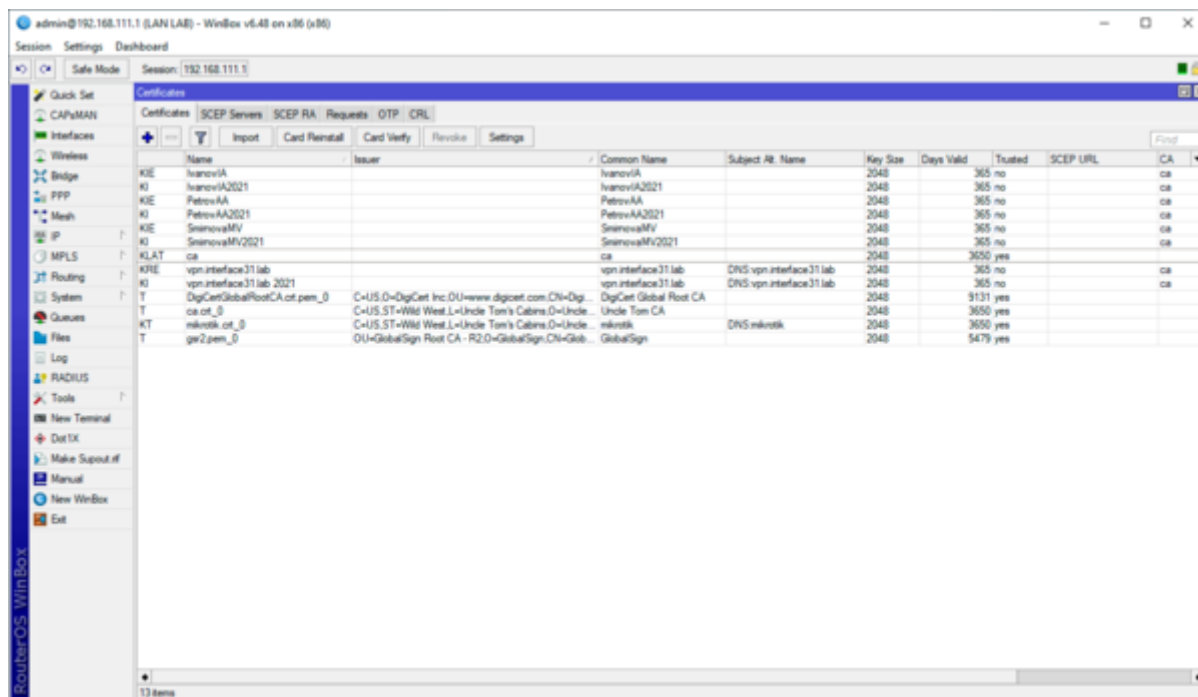
Следует понимать, что после того, как СА выпустил сертификат и передал его клиенту, он больше не может его контролировать и в случае компрометации его можно только отозвать. Между тем отозванный сертификат будет успешно проходить проверку подлинности при помощи корневого сертификата и проверить его на отзыв можно только при помощи списка CRL, который должен быть опубликован для общего доступа. Если CRL отсутствует или недоступен, то проверить сертификат на отзыв будет невозможно, а следовательно, такой сертификат будет принят как действительный.

В Mikrotik для работы с сертификатами следует перейти в отдельный раздел - **System - Certificates**. Прежде всего научимся правильно читать информацию о сертификатах, которая сосредоточена в первой колонке и представлена в виде буквенных флагов:

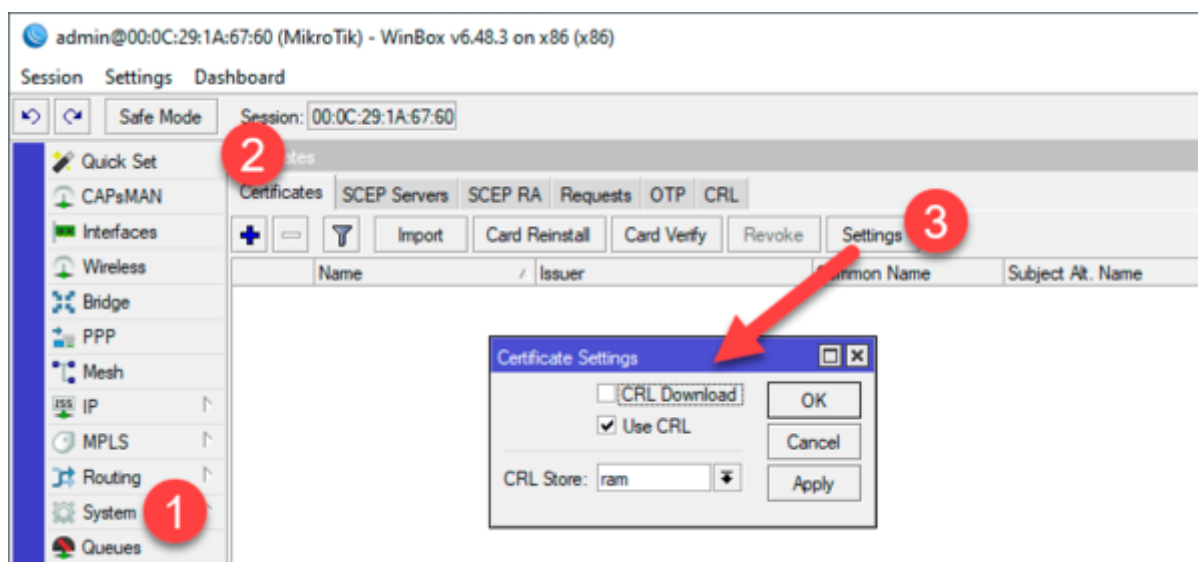
- **A - authority** - корневой сертификат при помощи которого мы можем подписывать другие сертификаты
- **T - trusted** - сертификат с которым установлены доверительные отношения
- **L - crl** - корневой сертификат содержит адрес списка отозванных сертификатов (CRL)
- **I - issued** - сертификат, выпущенный центром сертификации расположенном на данном устройстве
- **K - private-key** - сертификат имеет связанный с ним закрытый ключ
- **E - expired** - сертификат с истекшим сроком действия
- **R - revoked** - отозванный сертификат

Таким образом корневой сертификат СА должен иметь флаги **KAT** или **KLAT** в зависимости от того, использует ли центр сертификации списки отзыва CRL.

Выпущенный данным СА сертификат будет иметь флаг **KI**, а будучи импортированным на другом узле в присутствии сертификата СА будет иметь флаги **KT**, а сам корневой сертификат чужого СА - просто **T** или **LT**.



Закладка **System - Certificates - CRL** содержит загруженные списки отзыва для всех сертификатов, имеющих флаг **L**, кроме корневого сертификата собственного CA. Для работы со списками отзыва следует выполнить некоторые настройки, они расположены в **System - Certificates - Settings**. Флаг **Use CRL** включает использование списков отзыва, флаг **CRL Download** разрешает загрузку списков для сертификатов, содержащих адрес CRL. Если установить первый, но не устанавливать второй, то списки CRL будут работать только для собственного CA.

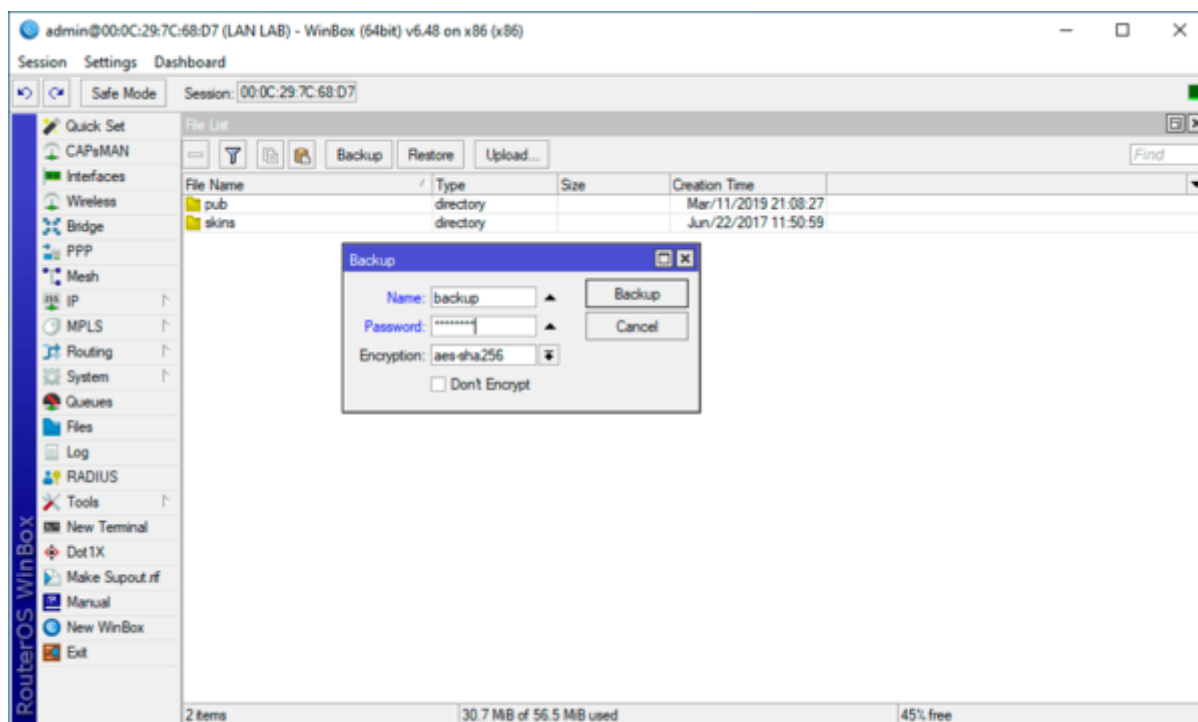


Еще одна важная опция - место хранения CRL - **CRL Store**, по умолчанию там стоит вариант хранения в оперативной памяти - **ram**. Но здесь есть первые подводные камни, объем RAM занимаемый списком рассчитывается по формуле:

$$4MB + 10 * <CRL\_size>$$

Таким образом даже самый небольшой список будет занимать от 4 МБ оперативной памяти, что может быть критично для младших моделей с небольшим объемом оперативной памяти, в этом случае значение **CRL Store** следует изменить на **system**.

Следующий важный вопрос: а что будет, если роутер с ролью СА выйдет из строя? В таком случае вы полностью потеряете контроль над своей PKI и вам потребуется создать новый СА и перевыпустить все сертификаты. Избежать этого можно только одним образом - созданием резервной копии устройства в бинарном формате. Для этого перейдите в **Files** и нажмите кнопку **Backup**, укажите имя файла и обязательно задайте пароль (в противном случае закрытые ключи выгружены в резервную копию не будут).



Либо выполните в терминале:

```
/system backup save name=backup password=<MY_PASSWORD>
```

Но бинарная копия имеет ряд существенных ограничений, она предназначена для восстановления только на том устройстве, на котором была создана, либо на другом той же модели при окончательном выходе устройства из строя. Это связано с тем, что при восстановлении такой копии будут восстановлены и MAC-адреса, а появление в одной сети двух устройств с одинаковыми MAC-адресами способно привести к серьезным сбоям в ее функционировании. Ну и наконец, вы не сможете восстановить бинарную резервную копию на другой модели роутера.

Этих недостатков лишена копия настроек в текстовом формате, которую можно полностью или частично восстановить на любом устройстве с RouterOS. Для ее создания выполните команду:

```
/export file=export_cfg
```

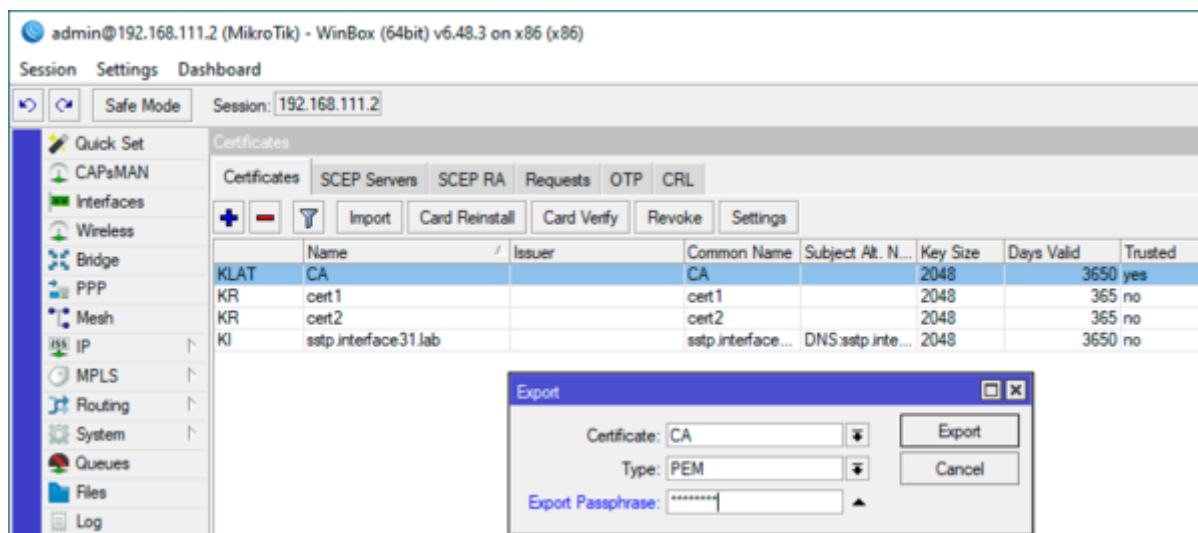
После чего в разделе Files у вас появится файл с указанным именем и расширением **.rsc**. Но данный файл не содержит ключей и сертификатов и не годится для восстановления СА. Скажем сразу - никаким иным способом, кроме как бинарным бекапом, перенести СА на другой роутер **нельзя**. Фактически центр сертификации получается в своем роде "одноразовым", его можно перенести только на точно такое же устройство, в случае апгрейда вам придется создать инфраструктуру PKI заново.

Но значит ли это, что вам не нужно делать резервную копию ключей и сертификатов? Нет. Никогда нельзя исключать внезапный выход роутера из строя, как и невозможность приобрести ему на замену точно такую же модель. А ситуация, когда все работает, хоть и с ограничениями, всегда лучше ситуации, когда не работает ничего.

Несмотря на то, что полноценно восстановить СА на другом узле мы не сможем, но работу служб, использующих сертификаты восстановить можно, хотя и с некоторыми оговорками. В некоторых случаях они могут оказаться существенными, почему так мы покажем ниже.

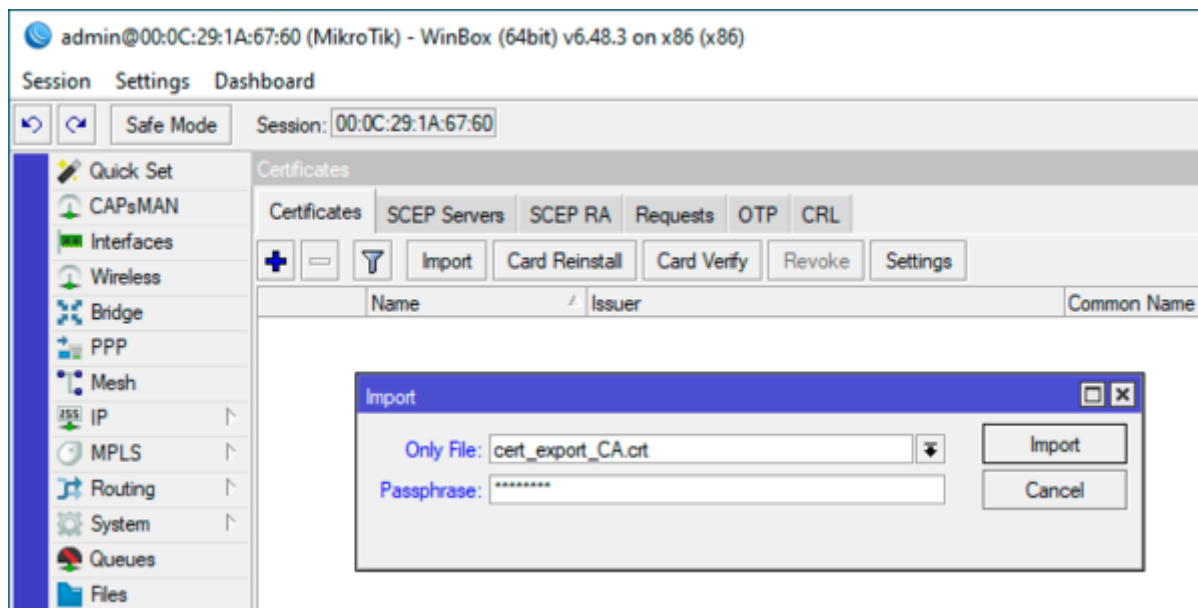
А пока экспортируем нужные нам ключи и сертификаты. Перейдем в **System - Certificates**, найдем там корневой сертификат СА и щелкнув на него правой кнопкой мыши выберем **Export**. Формат не имеет принципиального значения, при выборе **PEM** вы получите два файла - сертификат и закрытый ключ, при выборе **PKCS12** - единственный файл **.p12**.

Обязательно укажите пароль в поле **Export Passphrase**, в противном случае закрытые ключи выгружены не будут.

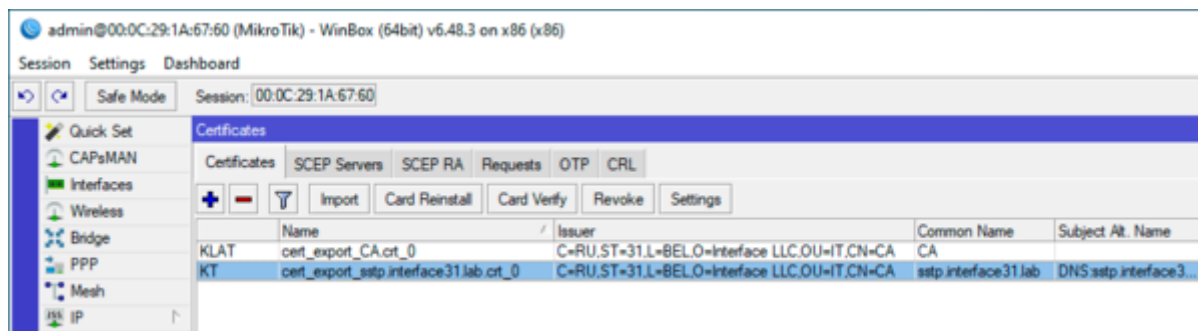


Затем, аналогичным образом, выгружаем сертификаты и ключи для служб, работающих на данном роутере, клиентские и серверные сертификаты, используемые на других узлах, выгружать не имеет смысла. Обратите внимание, так как выгружаемые ключевые пары содержат закрытые ключи, то следует обеспечить их безопасное хранение, особенно закрытого ключа центра сертификации СА.

При переходе на другое устройство вам потребуется загрузить сертификаты и ключевые пары, либо файлы **p12** в **Files**. После чего импортировать их в **System - Certificates**. Последовательность импорта такова: сначала сертификат, потом закрытый ключ, в случае файла **p12** все импортируется за одно действие.

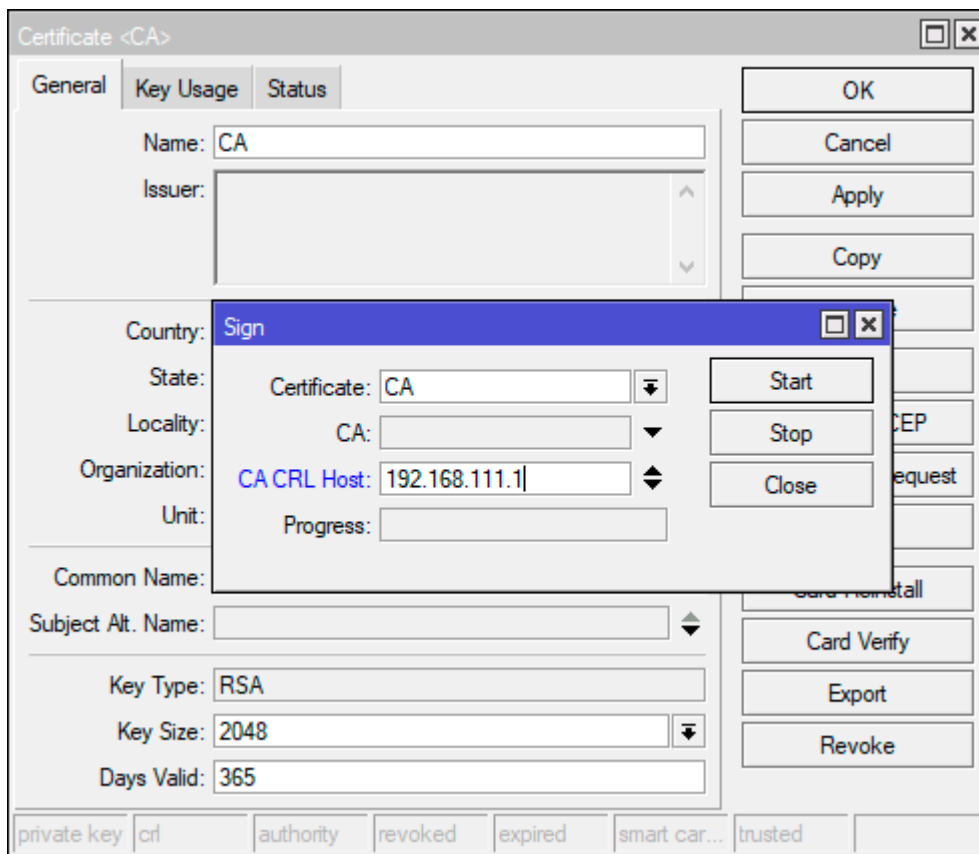


Глядя на статус импортированного корневого сертификата - **KLAT** - можно подумать, что все хорошо, но увы. Выпущенный этим же CA серверный сертификат импортируется не как **KI**, а как **KT**, это означает, что он будет работать, но отозвать мы его никогда не сможем, это же относится и к клиентским сертификатам, почему мы выше и сказали, что экспортировать их бессмысленно.



При этом вы можете продолжать выпускать сертификаты от имени CA и подписывать их корневым сертификатом. Если вы не используете в своей инфраструктуре PKI отзыв сертификатов, то можете продолжать работать. Никаких проблем при этом не возникнет.

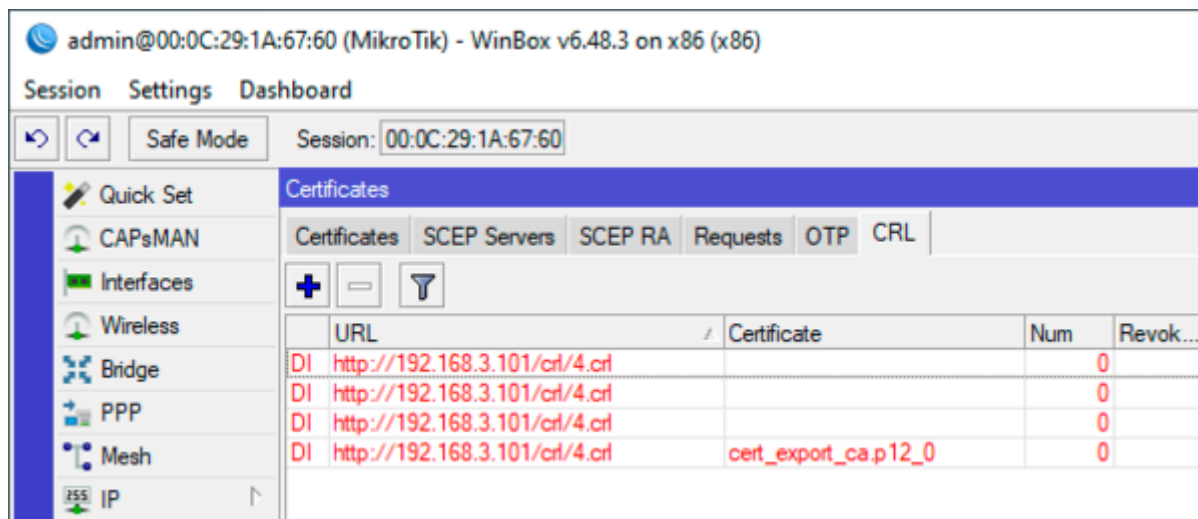
А мы тем временем перейдем к спискам отзыва, так как это самое больное место в этой схеме. При создании корневой ключевой пары CA, в момент подписи запрашивается адрес опубликования CRL - **CA CRL Host**, именно по этому адресу Mikrotik поднимет веб-сервер и опубликует список отозванных сертификатов.



Здесь снова есть подводные камни. Файл списка CRL при каждом изменении меняет свое название на номер итерации, так при первом создании он будет **http://192.168.111.1/crl/1.crl**, а после следующего отзыва превратиться в **http://192.168.111.1/crl/2.crl**. Адрес списка CRL содержится в корневом сертификате CA, поэтому, если вы используете несколько узлов, разрешающих доступ по сертификатам выпущенным Mikrotik, то после каждого отзыва вы должны заново экспортировать корневой сертификат CA и распространить его на все узлы вашей области доверия PKI, как минимум на те, которые принимают сертификаты для аутентификации или авторизации.

При переносе ключевой пары CA на другой хост RouterOS прочтает из корневого сертификата адрес CRL и попытается его скачать. Но так как старый роутер заменен новым, с тем же адресом, скачивать ему будет нечего. К сожалению, Mikrotik не позволяет импортировать файл списка CRL, поэтому даже имея его на руках вы не сможете загрузить его в устройство.





Но ведь мы можем выдавать новые сертификаты и можем их отозвать? Можем. Но новый список CRL при этом не формируется, центр сертификации будет продолжать пытаться загрузить список CRL указанный в корневом сертификате, которого в новом роутере не существует.

Таким образом, при переносе ключевой пары CA на новый роутер мы имеем возможность выдавать новые сертификаты, но сразу перестают действовать списки отзыва, т.е. клиенты с отозванными сертификатами снова могут подключиться к серверу, а также теряется возможность отзыва вновь выпущенных сертификатов.

Фактически старый CA перестал существовать, но мы можем продолжать поддерживать работоспособность текущей инфраструктуры PKI, хотя и с ограничениями, и планомерно планировать переход на сертификаты нового CA. Такой сценарий гораздо предпочтительнее, чем полный отказ инфраструктуры.

Как видим, в RouterOS нет возможности полноценно перенести CA на другое устройство, это серьезное ограничение и его следует обязательно учитывать при планировании инфраструктуры, в тоже время, располагая экспортированной ключевой парой CA и собственными сертификатами роутера вы всегда сможете восстановить работоспособность инфраструктуры, хотя и существенными ограничениями.

### Онлайн-курс по MikroTik

Научиться настраивать MikroTik с нуля или систематизировать уже имеющиеся знания можно на углубленном курсе по администрированию MikroTik. Автор курса, сертифицированный тренер MikroTik Дмитрий Скоромнов, лично проверяет лабораторные работы и контролирует прогресс каждого своего студента. В три раза больше информации, чем в вендорской программе MTCNA, более 20 часов практики и доступ навсегда.