Рабочий реестр TLS-сертификатов сайта

Пустой бланк — поля для заполнения обозначены в квадратных скобках.

Авторский проект образца. Адаптируйте условия и проверьте применимость перед использованием.

1. Номер, дата среза и область

Реестр является срезом наблюдения и назначений, а не автоматическим мониторингом. Укажите дату, область и источники списка конечных точек. Новый балансировщик или отдельный порт может предъявлять другой сертификат; нельзя объявлять все узлы проверенными по одному адресу главного сайта.

[Номер, дата среза и область]

2. Имена, порты, узлы и SNI

Для каждой конечной точки сохраните доменное имя, порт и узел, при необходимости способ выбора имени TLS. Соединение только по IP может получить другой сертификат. Совпадение DNS-адреса не гарантирует одинаковый результат на всех узлах и портах; непроверенные точки остаются отдельными открытыми строками.

[Имена, порты, узлы и SNI]

3. Идентификатор, отпечаток и издатель

Сопоставляйте сертификаты по устойчивому идентификатору и отпечатку с названным алгоритмом, а не только по похожему имени издателя. Публичный сертификат не является закрытым ключом, однако состав приложений всё равно проверяют. В реестр не помещают PEM закрытого ключа, пароли и ключ учётной записи ACME.

[Идентификатор, отпечаток и издатель]

4. Покрываемые имена и неподходящие адреса

Сохраните фактически проверенные имена расширения сертификата и результат сопоставления с нужной точкой. Нельзя считать любое поддоменное имя покрытым по наличию основного домена. Wildcard имеет свои границы; строку в реестре сверяют с данными сертификата, а не дополняют предполагаемыми удобными именами.

[Покрываемые имена и неподходящие адреса]

5. Начало, окончание и точка расчёта

Запишите notBefore и notAfter с известным часовым поясом и момент наблюдения. Дата окончания относится к конкретному сертификату, а не ко всему сервису. Самостоятельно введённая дата без чтения сертификата не является подтверждением; одинаковое число календарного дня в разных часовых поясах может означать разные моменты.

[Начало, окончание и точка расчёта]

6. Развёртывание и сравнение узлов

Сравните сертификат в конфигурации или файле и фактически предъявляемый при соединении. После замены файла процесс может продолжать выдавать прежнее состояние; это отдельная проверка. Не приписывайте результат одного узла всей группе, особенно при балансировке, разных именах и портах.

[Развёртывание и сравнение узлов]

7. Продление, владелец и подтверждённый прогон

Назовите владельца, механизм и реальный результат последней проверки продления без сохранения ключей. Наличие таймера или записи будущего срока не подтверждает успешную выдачу и развёртывание. Согласуйте, что делать при ошибке проверки домена; не отключайте проверку сертификата как обычный способ продлить его действие.

[Продление, владелец и подтверждённый прогон]

8. Предупреждения и эскалация

Определите пороги, адресатов и проверку доставки предупреждения по потребности сервиса. Порог является внутренним решением, а не свойством протокола TLS. При отсутствии ответственного предупредительный статус остаётся проблемой; отметка в таблице сама не отправляет сообщение и не выполняет продление.

[Предупреждения и эскалация]

9. Проверка доверия и открытые вопросы

Разделяйте сроки, совпадение имени, полноту цепочки и доверие клиента. Проверка даты не доказывает отсутствие отзыва, допустимость алгоритмов или безопасность приложения. Назовите фактически использованный инструмент и его ограничения; зелёная строка срока не является общим заключением о защищённости.

[Проверка доверия и открытые вопросы]

10. Следующие действия и история версий

Назначьте действия по каждой непроверенной точке и сохраните предыдущие срезы. Изменение сертификата требует фактической проверки предъявления на нужных узлах; старый результат не переносится на новый отпечаток автоматически. Исполнитель подтверждает наблюдавшиеся сведения, а не неограниченную будущую работоспособность сервиса.

[Следующие действия и история версий]