

Требования к настройке серверов имен при подтверждении права управления доменным именем

Настройка DNS

Автоматическая проверка права управления доменом (DCV) проводится в процессе выпуска TLS-сертификатов (для S/MIME применяется другой способ подтверждения). Сервис DCV ЦС TLS ТЦИ выполняет несколько запросов к серверам имён (NS), в том числе выполняет повторные запросы. Основой DCV при использовании DNS-проверки является размещение в TXT-записи строки с кодом, который выдаёт Центр Сертификации. При прохождении проверки по HTTP основное значение имеют А-записи (не поддерживаются AAAA-записи) и ответ веб-сервера.

Для успешного прохождения проверки (как DNS, так и HTTP-проверки) серверы имён (NS) и настройки DNS-зоны должны соответствовать требованиям RFC 1035, 1034, 1123, 2181, в частности:

1) должны быть согласованы списки делегирования зоны: то есть, в вышестоящей зоне присутствуют только имена NS, которые также указаны в списке NS делегируемой зоны;

2) список делегирования содержит как минимум два (различных) имени NS и данные имена указывают на как минимум два различных IP-адреса;

3) все NS, указанные в списке NS зоны, отвечают на запросы об именах в зоне с авторитативным статусом в ответе;

4) все авторитативные NS доступны по IPv4-адресам;

5) все авторитативные NS доступны по протоколу UDP (для v4) на номере порта 53;

6) все авторитативные NS доступны по протоколу TCP (для v4-адресов) на номере порта 53;

7) все авторитативные NS отвечают на запросы SOA и NS для DNS-зоны, содержащей проверяемое имя;

8) ответы авторитативных NS на запрос CAA-записей совпадают по составу (значению) записей;

9) ответы авторитативных серверов на запрос TXT-записей с кодом подтверждения DCV совпадают по значению проверяемой записи (то есть, TXT-запись с кодом подтверждения должна возвращаться в ответе каждого NS для зоны).

Настройка CAA-записей

CAA-запись – это DNS-запись, которая позволяет администратору опубликовать политики выпуска TLS-сертификатов для имён в зоне. В частности, администратор может явно разрешить выпуск сертификатов только конкретным УЦ (или всем УЦ). УЦ задаётся именем, которое указывается в CAA-записи. Формат и принципы использования CAA-записей определены в RFC 8659. Обычно используются опции issue и issuewild.

Пример CAA-записи:

```
google.com. IN CAA 0 issue "pki.goog"
```

Отсутствие CAA-записи в подходящей зоне разрешает выпуск сертификатов всем УЦ.

Для разрешения выпуска сертификатов ЦС TLS ТЦИ необходимо в CAA-записи указывать имя «tlscs.ru» (без кавычек).

ВАЖНО: для выпуска TLS-сертификата с wildcard-именем (*.test.ru) при наличии соответствующей CAA-записи ЦС ТЦИ требует непосредственного указания в дополнение к issue опции issuewild, разрешающей выпуск сертификатов ЦС ТЦИ. Отсутствие CAA-записи не препятствует выпуску сертификатов для wildcard-имён.

ЦС TLS ТЦИ проверяет наличие CAA перед выпуском сертификата, запрашивая в DNS CAA-записи, которые могут действовать для доменной зоны, указанной в заказе. Проверка CAA происходит до выполнения проверки права управления доменом (DCV). Если CAA запрещает выпуск сертификата, соответствующего заказу, то DCV не производится. Успешная проверка CAA не отменяет DCV: то есть, если в зоне размещена "разрешающая" CAA-запись, то размещать код подтверждения всё равно нужно. Для успешного прохождения проверки CAA ответы авторитативных серверов должны совпадать по составу CAA-записи.