Управление SSL сертификатами

Web-браузер взаимодействует с WCS по безопасному протоколу Secure Websockets для обмена сигнальными данными. Для передачи медиа данных используются WebRTC и Flash RTMFP технологии. В первом случае устанавливается безопасное соединение через DTLS с последующим обменом SRTP трафиком. RTMFP-протокол имеет встроенное шифрование AEC 128 бит. При взаимодействии с бэкендом и web-клиентами используется HTTPS.

Таким образом, управление безопасностью сервера сводится к настройкам, связанным с SSL - сертификатами

- Secure websockets
- HTTPS

RTMFP не требует дополнительных настроек, а сертификаты для DTLS генерируются автоматически при запуске сервера.

SSL сертификаты могут быть получены в любом центре сертификации, например, в Let's Encrypt.