

Аппаратное ускорение шифрования WebRTC трафика

По умолчанию, для шифрования WebRTC трафика используется библиотека [Bouncy Castle](#)

```
webrtc_aes_crypto_provider=BC
```

Однако, если процессор сервера поддерживает инструкции [AES](#), целесообразно переключиться на использование [Java Cryptography Extension](#) при помощи настройки в файле `flashphoner.properties`

```
webrtc_aes_crypto_provider=JCE
```

и включить поддержку AES в настройках JVM в файле `wcs-core.properties`

```
-server  
-XX:+UnlockDiagnosticVMOptions  
-XX:+UseAES  
-XX:+UseAESIntrinsics
```

В этом случае производительность шифрования за счет аппаратного ускорения увеличивается в 1,8-2 раза, что может снизить нагрузку на процессор сервера.

Проверить, поддерживает ли процессор сервера инструкции AES, можно при помощи команды

```
lscpu | grep -o aes
```

Если инструкции поддерживаются, команда выведет

```
aes
```

