WebRTC traffic encryption hardware acceleration

By default, Bouncy Castle library is used to encrypt WebRTC traffic

```
webrtc_aes_crypto_provider=BC
```

However, if AES instructions are supported by server CPU, it's recommended to enable Java Cryptography Extension usage with the following parameter in flashphoner.properties file

```
webrtc_aes_crypto_provider=JCE
```

and ennable AES support in JVM settings in wcs-core.properties file

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

In this case, encryption performance increases by 1,8-2 times due to hardware acceleration, that should decrease server CPU load average.

This command sholud be used to check if server CPU supports AES instructions

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

If the command prints

```
aes
```

it means AES instructions are supported