# Openssl获取ECC公私钥

**说明**：环境：ubuntu

获取的公钥要求：基于ECC的国密SM2算法的公私钥

**步骤1、**

**安装openssl**：在ubuntu或者其他linux上安装好openssl的版本，以下的网址是openssl最新的版本支持国密SM2

* [https://www.openssl.org/source/openssl-1.1.1-pre4.tar.gz](https://link.jianshu.com/?t=https%3A%2F%2Fwww.openssl.org%2Fsource%2Fopenssl-1.1.1-pre4.tar.gz)
* [https://www.openssl.org/source/openssl-1.1.1-pre5.tar.gz](https://link.jianshu.com/?t=https%3A%2F%2Fwww.openssl.org%2Fsource%2Fopenssl-1.1.1-pre5.tar.gz)

一般的ubuntu上已经有了openssl工具，但是可能不支持SM2。

## 检查椭圆曲线是否包含SM2

$ ./apps/openssl ecparam -list\_curves | grep SM2

SM2 : SM2 curve over a 256 bit prime field

所以以下的步骤是更新openssl的操作

1、查看源版本

[root@zj ~]# openssl version -a

OpenSSL 0.9.8e-fips-rhel5 01 Jul 2008

2、下载openssl-1.0.1g.tar.gz

wget http://www.openssl.org/source/openssl-1.1.1-pre4.tar.gz

3、更新zlib

yum install -y zlib

4、解压安装

tar zxf openssl-1.0.1g.tar.gz

cd openssl-1.0.1g

./config shared zlib

make

make install

mv /usr/bin/openssl /usr/bin/openssl.bak

mv /usr/include/openssl /usr/include/openssl.bak

ln -s /usr/local/ssl/bin/openssl /usr/bin/openssl

ln -s /usr/local/ssl/include/openssl /usr/include/openssl

echo “/usr/local/ssl/lib” >> /etc/ld.so.conf

ldconfig -v

5、查看是否升级成功

[root@zj ~]# openssl version -a

OpenSSL 1.1.1-pre4 7 Apr 2018

**步骤2、**

## 生成SM2私钥

$ openssl ecparam –genkey –name SM2 –out priv.key

## 显示私钥的内容：包含公钥和私钥的内容

$ openssl ec –in priv.key -text

将公钥写入文件：

openssl ec -in eckey.pem -pubout -out ecpubkey.pem

显示密钥信息：

1. openssl ec -in eckey.pem –text
2. openssl ec -in ecpubkey.pem -pubin –text

-