OpenSSL相关命令（forLinux）详细介绍 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/240/2021_2022_OpenSSL_E7_9B_B8_c103_240659.htm 加密算法： 对称加密算法： DES、IDEA、RC2、RC4、AES、Skipjack …… 非对称加密算法：RSA、DSA、DiffieHellman、PKCS、PGP …… 单向的HASH算法属于报文摘要算法，虽然有些也出自OpenSSL库。 命令操作： 1、生成普通私钥：[weigw@TEST src]$ openssl genrsa -out privatekey.key 1024Generating RSA private key, 1024 bit long modulus .... e is 65537 (0x10001) 2、生成带加密口令的密钥：[weigw@TEST src]$ openssl genrsa -des3 -out privatekey.key 1024Generating RSA private key, 1024 bit long modulus .... e is 65537 (0x10001) Enter pass phrase for privatekey.key: Verifying - Enter pass phrase for privatekey.key: 在生成带加密口令的密钥时需要自己去输入密码。对于为密钥加密现在提供了一下几种算法：-des encrypt the generated key with DES in cbc mode -des3 encrypt the generated key with DES in ede cbc mode (168 bit key) -aes128, -aes192, -aes256 encrypt PEM output with cbc aes 去除密钥的口令：[weigw@TEST src]$ openssl rsa -in privatekey.key -outprivatekey.key Enter pass phrase for privatekey.key: writing RSA key 通过生成的私钥去生成证书：[weigw@TEST src]$ openssl req -new -x509 -key privatekey.key -out cacert.crt -days 1095You are about to be asked to enter information that will be incorporated into your certificate request.What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some

blank For some fields there will be a default value, If you enter ., the field will be left blank.-----Country Name (2 letter code) [GB]:CN State or Province Name (full name) [Berkshire]:beijing Locality Name (eg, city) [Newbury]:beijing Organization Name (eg, company) [My Company Ltd]:wondersoftOrganizational Unit Name (eg, section) []:develop Common Name (eg, your name or your servers hostname) []:WeiGWEmail Address []:weigongwan@sina.com 在生成证书的时候需要按照提示输入一些个人信息。 通过私钥生成公钥：[weigw@TEST src]$ openssl rsa -in privatekey.key -pubout -out pubkey.key writing RSA key 格式转换：（证书、私钥、公钥）（PEM DER ）[weigw@TEST src]$ openssl x509 -in cacert.crt -inform PEM -out cacert.der -outform DER [weigw@TEST src]$ [weigw@TEST src]$ openssl rsa -in privatekey.key -inform PEM -out privatekey.der -outform DER writing RSA key[weigw@TEST src]$ openssl rsa -pubin -in pubkey.key -inform PEM -pubout -out pubkey.der -outform DER writing RSA key从DER格式转换成PEM格式一样，就是把inform的格式改成DERoutform的格式改成PEM即可。