some terms in IPsec support

During the STC integration test with Huawei IPsec GW, service engineers seem lack understanding of terms. So I give some short description here.

What is the CA:

Digital signatures are widely used is in certificate management.
e.g
If Alice is willing to validate Bob's certificate, she can sign it with her private key. Once she's done that, Bob can attach her signature to his certificate. Now, let's say he gives the certificate to Charlie, and Charlie does not know that Bob actually gave him the certificate, but he would believe Alice if she told him the certificate belonged to Bob. In this case, Charlie can validate Alice's signature, thereby demonstrating that the certificate does indeed belong to Bob.

standards

- PKCS: by RSA, for certifcate
  Here we mainly use PKCS#1, PKCS#7
  and the PKCS#7 is compatible with PEM.
- OCSP (Online Certificate StatusProtocol): by IETF
  to check the validity of certifcate

how to sign a certifcate in eNB

```
crasign [-d digest=md5|sha1|sha224|sha256|sha384|sha512|ripemd160] [-k key-chain=/etc/keys.d/private/sok.crk&sig.
```