# ECC avec OpenSSL

Pour voir la liste des ciphers ECC

* openssl ciphers –v | grep EC

Pour générer une clé (un fichier qui contient la clé publique et la clé privée), ensuite il faut extraire la clé publique de ce fichier

* openssl ecparam –out key.pem –name prime256v1 –genky
* On peut utiliser d’autres taille de la clé : openssl ecparam –list\_curves
* prime256v1 : pour 256 bits
* secp384r1 : pour 384 bits
* sec512r1 : pour 512 bits

Pour extraire la clé publique

* openssl ec -in key.pem -pubout -out public.pem

Pour signer un fichier data.txt qui contient “my data” ou mettre echo directement

* echo  “my data” | openssl dgst –ecdsa-with-SHA1 –sign key.pem –out signature.bin
* voir le résultat

Pour verifier la signature avec la clé publique

* openssl dgst –sha1 –verify public.pem -signature signature.bin data.txt
* il doit afficher VERIFIED OK

Pour générer le certificat de la CA

* openssl ecparam -out ca-key.pem -genkey -name prime256v1
* openssl req -x509 -new -key ca-key.pem -out ca-cert.pem

Pour formuler la requette de la demande .csr du serveur

* openssl ecparam -out server-key.pem -genkey -name prime256v1 –noout
* openssl req -new -key server-key.pem -out server-csr.pem

Signature de la demande du serveur par la clé privée de la CA

* openssl x509 -req -days 365 -in server-csr.pem -CA ca-cert.pem -CAkey ca-key.pem -set\_serial 01 -out server-cert.pem
* il doit afficher
  + Signature ok
  + Subject=/C=fr/ST=serveur rida/L=paris/0=mon entreprise/OU=entr/CN=www.rida.fr
  + Getting CA Private Key