

Cryptographie Courbes elliptiques

■ ■ ■ Chiffrement ECC : clés et certificats

Pour la génération de l'AC, il est possible de passer directement en ligne de commande les différents paramètres de l'AC :

```
xterm
$ openssl ecparam -out ecc.ca.key.pem -name prime256v1 -genkey

$ openssl req -config <(printf
"[req]\ndistinguished_name=dn\n[dn]\n[ext]\nbasicConstraints=CA:TRUE") -new -nodes
-subj "/C=FR/L=Limoges/O=CRYPTIIS/OU=SecuTIC/CN=ACSECUTIC" -x509 -extensions ext
-sha256 -key ecc.ca.key.pem -text -out ecc.ca.cert.pem
```

Pour la génération d'un certificat pour un serveur :

```
xterm
$ openssl ecparam -out ecc.key.pem -name prime256v1 -genkey

$ openssl req -config <(printf
"[req]\ndistinguished_name=dn\n[dn]\n[ext]\nbasicConstraints=CA:FALSE") -new -subj
"/C=FR/L=Limoges/O=CRYPTIIS/OU=SecuTIC/CN=serveur" -reqexts ext -sha256 -key
ecc.key.pem -text -out ecc.csr.pem

$ openssl x509 -req -days 3650 -CA ecc.ca.cert.pem -CAkey ecc.ca.key.pem
-CAcreateserial -extfile <(printf "basicConstraints=critical,CA:FALSE") -in
ecc.csr.pem -text -out ecc.serveur.pem
```

Questions :

- Comparez la taille des clés et certificats basés ECC par rapport à des clés et certificats basés RSA ;
- Testez à l'aide d'openssl «s_client» et «s_server» l'authentification par certificats basés ECC.
- Quels sont les paramètres recommandés pour l'usage actuel du chiffrement ECC ?
- Qu'est-ce que vous pouvez apprendre de la RFC 7748 ?
Quel rapport entre «Curve25519» et «NIST P-256», aka «prime256v1» ?
- Si vous lisez <https://tools.ietf.org/html/draft-irtf-cfrg-curves-02>, quelles sont les «Recommended Curves» ?

Demandez la liste des courbes elliptiques gérées dans openssl :

```
xterm
openssl ecparam -list_curves
```

Que pouvez-vous en déduire ?
Est-ce prévu à l'avenir ?