OpenSSL - sess_id

Utilitaire pour manipuler et afficher les ID de session SSL/TLS

OPTIONS

-inform DER|PEM Format d'entrée

-outform DER|PEM Format de sortie

-in filename Fichier d'entrée contenant les informations de session

-out filename Fichier de sortie où écrire les informations de session

-text Affiche les composante clé privée et publique en texte clair en plus de la version encodée

-cert Si un certificat est présent dans la session il sera sortie, si -text il sera affiché

-noout Ne sort pas la version encodée de la session

-context ID Spécifie l'id de session

Sortie

```
SSL-Session :
Protocol : TLSv1
Cipher : 0016
Session-ID : 871E62626C554CE95488823752CBD5F3673A3EF3DCE9C67BD916C809914B40ED
Session-ID-ctx : 01000000
Master-Key : A7CEFC571974BE02CAC305269DC59F76EA9F0B180CB6642697A68251F2D2BB57E51DBBB4C7885573192AE9AEE220FACD
Key-Arg : None
Start Time : 948459261
Timeout : 300 (sec)
Verify return code 0 (ok)
```

Détails

Protocol Protocole utilisé (TLSv1, SSLv2 ou SSLv3)

Cipher Chiffrement utilisé

Session-ID L'id de session en hexa

Session-ID-ctx Contexte de l'id de session en hexa

Master-Key Clé maître de session SSL

Key-Arg Argument clé, utilisé en SSLv2

Start Time Heure de début de la session au format Unix standard

Timeout timeout en secondes

Verify return code code de retour quand le certificat client est vérifié

Notes

La version PEM du fichier de session utilise :

```
---BEGIN SSL SESSION PARAMETERS---
---END SSL SESSION PARAMETERS---
```