
OpenSSL - dgst

Afficher le message digest en hexa d'un ou plusieurs fichiers. Peut également être utilisé pour les signatures numérique et la vérification.

OPTIONS

- c Affiche le digest en 2 groupes de chiffre séparés par un ' : '
- d Affiche des informations de debuggage BIO
- hex Affiche le digests en tant que dump hexa. Défaut pour les digest normaux en opposé aux signatures numériques.
- binary Affiche le digest au format binaire
- out filename Nom du fichier de sortie
- sign filename Signe numérique le digest en utilisant la clé privée dans le fichier spécifié.
- keyform PEMENGINE Spécifie le format de la clé pour signer le digest.
- engine id Utilise l'id pour les opérations (incluant le stockage de la clé privée). Ce moteur n'est pas utilisé comme source pour les algorithmes digest, à moins qu'il soit également spécifié dans le fichier de configuration
- sigopt nm :v Passer des options à l'algorithme de signature durant les opérations de signature et de vérification.
- passing arg Mot de passe de la source du mot de passe.
- verify filename Vérifie la signature en utilisant la clé publique dans le fichier spécifié.
- prverify filename Vérifie la signature en utilisant la clé privée dans le fichier spécifié.
- signature filename La signature à vérifier
- hmac key Créé un MAC hashé en utilisant la clé spécifiée.
- mac alg Créer un MAC en utilisant l'algorithme spécifié.
- macopt nm :v Passer des options à l'algorithme MAC
- rand file(s) Spécifier le(s) fichier(s) à utiliser pour le générateur de nombre aléatoire, ou un socket EGD.
- file... Fichier en entrée pour les opération de digest.