/etc/moduli

moduli Diffie-Hellman

Le fichier /etc/moduli contient les nombre premier et générateurs pour sshd lors de l'échange de clé Diffie-Hellman.

Un nouveau moduli peut être généré par ssh-keygen en utilisant un processus à 2 étapes. Un pass initial de génération candidat, utilisant ssh-keygen -G, calcule les nombres qui sont utiles. Puis une passe test, utilisant ssh-keygen -T, fournis au haut niveau d'assurance que les nombres sont premiers et sont sûre pour les opérations DH. Le format moduli est utilisé comme sortie depuis chaque passe.

Le fichier consiste d'enregistrement, un par modulo, contenant 7 champs :

timestamp La date du traitement du modulus

type Spécifie la structure interne (0=inconnu, non testé, 2=safe prime, 4=Sophie Germain)

tests Indisque le type de tests de primalité (0x00=non testé,0x01=nombre composite, pas premier, 0x02=Sleve of Eratosthenes, 0x04=Probabilistic Miller-Rabin primality tests)

trials Nombre de primalité effectués dans le modulus

size Taille du prime en bits

generator Le générateur recommandé à utiliser avec ce modulus (en hexa)

modulus Le modulus lui-même en hexadécimal