Deutsch

OTT netDL – Hinweise zur verschlüsselten Datenübertragung

HTTPS Übertragungsprotokoll

- Unterstützte Verschlüsselungsprotokolle: **SSL 3.0** sowie **TLS 1.0, TLS 1.1, TLS 1.2**
- Mögliche Schlüssellängen: **512 ... 2048 Bit**
- Unterstützte **„Cipher Suites“** [1]:
  - RSA_WITH_AES_128_CBC_SHA
  - RSA_WITH_AES_256_CBC_SHA
  - RSA_WITH_AES_256_CBC_SHA256
  - RSA_WITH_3DES_EDE_CBC_SHA
  - RSA_WITH_RC4_128_SHA
  - RSA_WITH_RC4_128_MD5
  - RSA_WITH_NULL_MD5
  - RSA_WITH_NULL_SHA

Bitte beachten

- Der OTT netDL unterstützt **keine ECDH[2] - oder DH[3] -Algorithmen!**
- Der OTT netDL unterstützt **kein SFTP oder FTP-S!**

[1] standardisierte Chiffrensammlungen für Verschlüsselungsalgorithmen
[2] ECDH: Elliptic Curve Diffie-Hellman; kryptografisches Schlüsselaustauschprotokoll
[3] DH: Diffie-Hellman; kryptografisches Schlüsselaustauschprotokoll

English

OTT netDL – Notes on encrypted data transmission

HTTPS transmission protocol

- Supported encryption protocols: **SSL 3.0** as well as **TLS 1.0, TLS 1.1, TLS 1.2**
- Possible key lengths: **512 ... 2048 Bit**
- Supported **„Cipher Suites“** [1]:
  - RSA_WITH_AES_128_CBC_SHA
  - RSA_WITH_AES_256_CBC_SHA
  - RSA_WITH_AES_256_CBC_SHA256
  - RSA_WITH_3DES_EDE_CBC_SHA
  - RSA_WITH_RC4_128_SHA
  - RSA_WITH_RC4_128_MD5
  - RSA_WITH_NULL_MD5
  - RSA_WITH_NULL_SHA

Please note

- The OTT netDL does **not support ECDH[2] or DH[3] algorithms!**
- The OTT netDL does **not support SFTP or FTP-S!**

[1] standardized cipher collections for encryption algorithms
[2] ECDH: Elliptic Curve Diffie-Hellman; cryptographic key exchange protocol
[3] DH: Diffie-Hellman; cryptographic key exchange protocol

OTT Hydromet GmbH

Ludwigstrasse 16
87437 Kempten · Germany
Phone +49 831 5617-0
Fax +49 831 5617-209

info@ott.com · www.ott.com

55.552.001.I.M 01-0817