Deutsch

OTT netDL – Hinweise zur verschlüsselten Datenübertragung

HTTPS/MQTTS/FTPS Übertragungsprotokoll

- Unterstützte Verschlüsselungsprotokolle: **TLS 1.2**
- Mögliche Schlüssellängen: **512 ... 4096 Bit**
- Unterstützte **„Cipher Suites“** [1]:
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 [2]
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 [2]
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA [2]
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA [2]

Bitte beachten

- Gültig für OTT netDL Firmware **V 3.07.0** oder höher!
- **FTPS:** Server muss für **PROT C** konfiguriert sein (keine Unterstützung von PROT P)!
- Der OTT netDL unterstützt **kein SFTP!**

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

English

OTT netDL – Notes on encrypted data transmission

HTTPS/MQTTS/FTPS transmission protocol

- Supported encryption protocols: **TLS 1.2**
- Possible key lengths: **512 ... 4096 Bit**
- Supported **„Cipher Suites“** [1]:
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 [2]
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 [2]
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA [2]
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA [2]

Please note

- Valid for OTT netDL Firmware **V 3.07.0** or higher!
- **FTPS:** Server must be configured for **PROT C** (no support of PROT P)!
- The OTT netDL does **not support SFTP!**

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

55.552.001.I.M 04-0824

OTT HydroMet GmbH
Ludwigstrasse 16
87437 Kempten · Germany
Telephone +49 831 5617-0
Fax +49 831 5617-209
euinfo@otthydromet.com
www.otthydromet.com