



OTT netDL – Hinweise zur verschlüsselten Datenübertragung

HTTPS/MQTT/FTPS Übertragungsprotokoll

- ▶ Unterstützte Verschlüsselungsprotokolle: **TLS 1.2**
- ▶ Mögliche Schlüssellängen: **512 ... 4096 Bit**
- ▶ Unterstützte „**Cipher Suites**“¹⁾:
 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256²⁾
 - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256²⁾
 - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA²⁾
 - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA²⁾

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

Deutsch

OTT netDL – Notes on encrypted data transmission

HTTPS/MQTT/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_SHA256²⁾
 - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256²⁾
 - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA²⁾
 - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA²⁾

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

English

55.552.001.1.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