

# *Mega\_Link 2*

## *APPLICATION NOTE AN045*

### *Using Mega\_Link 2 with AES-256 Encryption & Retrofit Compatibility*

#### **Summary**

Mega\_Link 2 is a versatile and secure radio telemetry system for passing instrumentation, measurement and control data between industrial plants and different site locations.

All transmitted data streams are encrypted using the AES-256 encryption standard in response to the UK implementing the Network and Information Systems Regulations (NIS).

By implementing and adopting Mega\_Link 2 with AES-256 encryption, organisations can demonstrate their commitment; to data security and to meeting the requirements of NIS and Cyber Assessment Framework (CAF).

Mega\_Link 2 has flexible built-in communications modes include;

UHF Low Power Radio (458MHz and 869MHz, licence exempt)

4G Mobile Networks (User or Churchill provided SIM cards)

TCP/IP Ethernet for local area networks

External modems, e.g. Licenced Frequencies, ADSL/DSL, Fibre Optic, Satellite etc.

Mega\_Link 2 provides an easy and cost-effective upgrade and swap-out path from the previous generations of Mega\_Link 1, Micro\_Link and Nano\_Link telemetry products.

This application note explains the benefits of using AES-256 encryption of and the retrofit compatibility aspects of Mega\_Link 2.

## *Using Mega\_Link 2 with AES-256 Encryption*

### **Mega\_Link 2 Operation**

Mega\_Link 2 is intended for use as a local telemetry and control system either operating stand-alone or on the periphery of a utility companies' wider network of telemetry and control infrastructure.

A typical Mega\_Link 2 application comprises a basestation and one or more associated outstations. The basestation communicates with each outstation in turn to exchange digital and analogue measurement and control signals.

Fundamentally, Mega\_Link 2 is used to exchange 4-20mA analogue and discrete digital signals between different locations over a transmission link, in a peer to peer arrangement; physical signals go in one end and are relayed to come out at the other end of the link.

These low-level signals are normally interfaced to customer specific equipment at the analogue and digital hard-wired physical level and can also be interfaced to PLC/SCADA systems using serial Modbus RTU or similar.

Mega\_Link 2 incorporates industry standard AES-256 encryption for secure communications of the messages which represent the analogue and digital signal data whilst in-transit "over the air" between the basestation and outstation(s). For communications media options, see later section.

### **Mega\_Link 2 AES-256 Encryption**

Mega\_Link 2 incorporates AES-256 encryption for secure communications between basestation and outstation(s).

AES-256 is a highly secure symmetric encryption algorithm, developed by the National Institute of Standards and Technology (NIST), that uses a 256-bit key to encrypt data, making it virtually unbreakable for current computing capabilities.

Mega\_Link2 is based around a Renesas S5D9 Synergy family MCU which incorporates a Secure Cryptographic Engine (SCE7) module to provide security functions. This "hardware encryption engine" module consists of an access management circuit, encryption engine and random number generator. In combination with the Renesas Synergy Software Package (SSP) Crypto library, the SCE7 can prevent eavesdropping (confidentiality), falsification of information (integrity), and impersonation (authenticity).

Encryption engine Advanced Encryption Standard (AES): Compliant with NIST FIPS PUB 197 algorithm.

- Key size: 256 bits
- Block size: 128 bits
- Chaining modes
  - ECB, CBC, CTR: Compliant with NIST SP 800-38A
  - GCM: Compliant with NIST SP 800-38D
  - XTS: Compliant with NIST SP 800-38E
  - GCTR.

### **NIS Cyber Security Compliance Strategy**

In the context of the Network and Information Security Directive 2 (NIS2) and UK cybersecurity, AES-256 encryption is a widely recognized and robust method for protecting data, ensuring compliance with the directive's stringent security requirements, especially for essential and important entities.

Churchill Controls Ltd. Unit 30 Wellington Business Park, Dukes Ride, Crowthorne, RG45 6LS  
Tel: +44 (0)1344 750233 e-mail: [sales@churchill-controls.co.uk](mailto:sales@churchill-controls.co.uk)

## ***Using Mega\_Link 2 with AES-256 Encryption***

By implementing and adopting Mega\_Link 2 with AES-256 encryption, organisations can demonstrate their commitment; to data security and to meeting the requirements of NIS and Cyber Assessment Framework (CAF).

### **AES-256 Key Management**

When new, the Mega\_Link 2 equipment is shipped to a customer with a default or “factory” encryption key. If requested it can also be supplied pre-installed with a customer specific encryption key instead. Obviously, this will then be known to Churchill Controls.

After delivery, the USB interface can be used with a laptop running a small utility programme to download a new custom encryption key file. After commissioning, it is recommended that customers should install their own “known only by them” encryption key file and then periodically update or rotate keys according to their company’s NIS key management procedures.

### **PIN Code for LCD User Interface**

The Mega\_Link 2 has a built in LCD screen with joystick to be used for monitoring operation via a menu of available functions. As standard, all menu items that can change or alter normal operation, e.g. Calibration, Radio Frequency etc. are PIN code protected.

For units that are installed in non-secure locations, then the display option can either be deleted or upon request Mega\_Link 2 can be supplied with PIN code protection required to control operation of all display functions.

### **Password Protection on USB Interface for Configuration and Diagnostics**

The Mega\_Link 2 has a USB interface for a laptop running DCD2 software to be used for configuration programming and diagnostics. If requested, this can have the option to be password protected.

### **Replacing or Upgrading Mega\_Link 1 and Legacy Equipment**

Mega\_Link 2 follows the same functional and operational requirements as our existing family of products, hence minimising the cost of replacement and upgrade of previous generations of Mega\_Link 1, Micro\_Link and Nano\_Link low power radio equipment.

The Mega\_Link 2 physical dimensions and mounting arrangement of the main unit is identical to Mega\_Link 1.

The Mega\_Link 2 power, aerial, I/O and Fieldbus connectors and interface characteristics on the main unit are directly backward compatible with Mega\_Link 1.

The Mega\_Link 2 I/O expansion modules will however require some re-wiring to a different style of connector in order to replace existing Mega\_Link 1 expansion units.

### **4G LTE Cellular Network Operation**

Where the use of low power radio is not possible or desirable then the 4G cellular network option comes

Churchill Controls Ltd. Unit 30 Wellington Business Park, Dukes Ride, Crowthorne, RG45 6LS  
Tel: +44 (0)1344 750233 e-mail: [sales@churchill-controls.co.uk](mailto:sales@churchill-controls.co.uk)

## *Using Mega\_Link 2 with AES-256 Encryption*

into play. Still with AES-256 encryption while traversing through the cellular networks. 4G Mega\_Link 2 can be operated with customer supplied SIM cards with fixed IP and peer to peer capability enabled or else Churchill can supply SIM cards with two-yearly data allowance, payable every two years.

### Transmission Media Options

#### Single Comms

Comms Media	Primary	Bus_Link
Radio	COM1 (RC458)	COM3A or COM3B
4G LTE	COM1 (4G)	COM3A or COM3B
RS232 external modem	COM3A (RS232)	Not available
RS485 external modem	COM3B (RS485)	Not available
Ethernet TCP/IP Local Network or external modem	COM4 (Ethernet)	COM3A or COM3B

#### Dual Comms

Comms Media	Primary	Secondary	Bus_Link
Radio + Radio	COM1 (RC458)	COM2 (RC458)	COM3A or COM3B
4G LTE + Radio	COM1 (4G)	COM2 (RC458)	COM3A or COM3B
Radio + RS232 external modem	COM1 (RC458)	COM3A (RS232)	Not available
Radio + RS485 external modem	COM1 (RC458)	COM3B (RS485)	Not available
Radio + Ethernet TCP/IP Local Network or external modem	COM1 (RC458)	COM4 (Ethernet)	COM3A or COM3B

#### Key:

RC458 = 458MHz Licence Exempt Low Power Radio

4G LTE = Local Network (TCP/IP)

Ethernet = Local Network (TCP/IP)

#### Bus\_Link/Fieldbus:

Modbus (RTU)	Master	RS232/RS485
Modbus (RTU)	Slave	RS232/RS485
Allen Bradley DF1	Master	RS232/RS485
Allen Bradley DF1	Slave	RS232/RS485

End.

Churchill Controls Ltd. Unit 30 Wellington Business Park, Dukes Ride, Crowthorne, RG45 6LS  
 Tel: +44 (0)1344 750233 e-mail: [sales@churchill-controls.co.uk](mailto:sales@churchill-controls.co.uk)