SUPERFLEX™

The IDC FLEXROUTE IP Pro Audio Suite — true end-to-end solutions for the distribution of broadband multimedia content via satellite

HEAD END | RECEIVERS | MANAGEMENT & CONTROL | CONTENT DISTRIBUTION

FLEXKEY ENCRYPTOR

DVB CAS SYSTEM

FEATURES:

- High speed encryption of DVB Transport Stream packets – up to 181 Mb/s and 128-bit AES encryption.
- DVB/ASI input and output, with auto-lock to 188 or 204 byte DVB transport format.
- Redundant DVB/ASI inputs A and B with auto-sensing.
- All selected PIDs encrypted using the same key
- 56/64 bit blowfish/DES optional
- Keys can be cycled over a specified period of time (even, odd) from 2 minutes to 1 week.
- Locally configurable via a serial terminal interface.
- Remotely configurable and upgradeable using password protected web interface.
- Front panel LED indicators provide easy operational status.
- Linux based O/S for reliable and stable operation.
- Support for multiple languages (English currently supported).
- Local or remote logging.

The FlexKey Encryptor is IDC's own low cost, flexible key DVB CAS system, which encrypts selected PID data within a DVB Transport Stream destined for the Superflex series of satellite receivers: the SR2000plus, SR2000pro, Sxx2100F series, SRA2100f and SFX2100f.

Installed at the head end, it's placed between the DVB IP Encapsulator (IPE) and the DVB Modulator. It receives an ASI transport stream from the IPE, encrypts DVB packets for selected PIDs and forwards the resulting transport stream out another ASI interface to the modulator. The user monitors and controls the FlexKey Encryptor with a Web GUI or Terminal Interface. Front panel LED indicators are also provided.

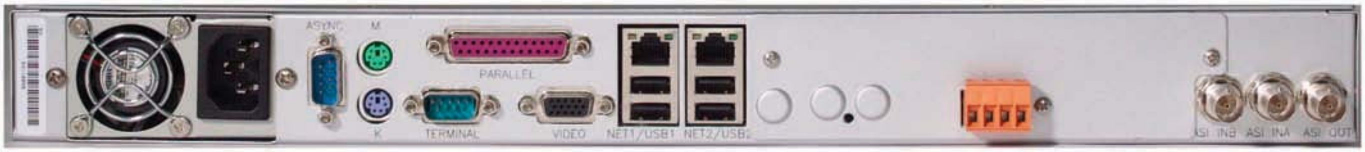
KEY GENERATION – using a sophisticated random number generation algorithm, and passed onto an internal secure device for encryption. Keys are encrypted using a security device which has an internal "secret", programmed at the factory. It must also be programmed into the security device of each receiver that wishes to decrypt the data on the network. The "secret" itself is also encrypted for highly secure operation.

KEY MANAGEMENT – supports key pairs (i.e. even and odd keys) using a mechanism similar to that used to manage keys in DVB CAS. Encrypted keys are communicated to the receivers using Entitlement Control Messages (ECMs).

Two parameters are associated with key management. The ECM Transmission Period indicates how often ECMs are sent out and the Key Update Period determines how often the keys in the ECM are changed. Keys can be updated automatically or manually.

DATA ENCRYPTION – selected DVB packets are encrypted using the AES Rijndael algorithm, using the associated even or odd 128-bit key. It sets the scrambled bits in the header of each DVB packet to indicate which key (even or odd) was used to encrypt that packet, as is done with DVB CAS. The same key, even or odd, is used to encrypt all selected PIDs.

SUPERFLEX



TECHNICAL SPECIFICATIONS

FRONT PANEL INDICATORS

Lock: Indicates frame sync to either A or B ASI input

Status: Indicates normal operation or system failure

Even/Odd: Indicates which key (even or odd or none) is being used for encryption

RW: Indicates storage device activity

Enc Mode: Indicates which Encryption Mode is being used

ECM: Indicates data activity on the ECM transmission stream

Key Mode: Indicates whether keys are updated manually or automatically

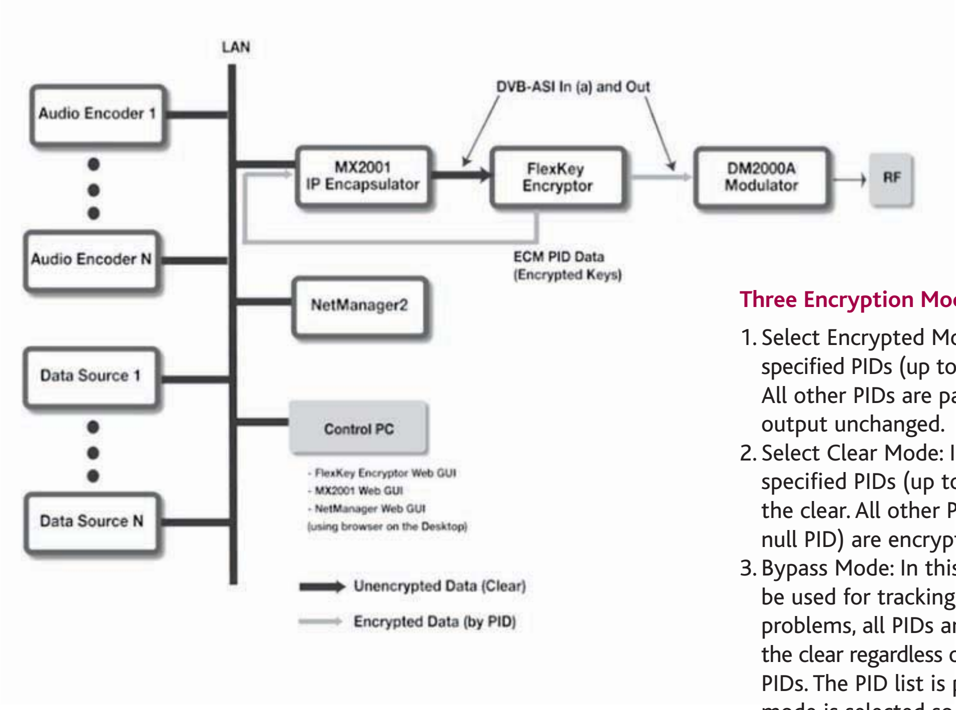
Option 1: Reserved for future options

REAR PANEL CONNECTORS/INDICATORS

- Keyboard/Monitor/Mouse for local console use
- 1 Serial terminal interface port
- 1 Asynchronous COM type port for future options
- 1 Parallel port for future options
- 2 Ethernet 10/100 Base-T ports
- 4 USB ports for future options
- 2 DVB/ASI Input Ports
- 1 DVB/ASI Output Port
- 1 Form-C Status Relay contacts on a screw terminal strip

PHYSICAL PARAMETERS

Chassis:	1 Rack Unit (RU) height
Dimensions:	4 cm H x 36 cm D x 48 cm W
Weight:	Less than 7 kg
Supply Voltage:	100 to 240 VAC ±10%, 50 or 60 Hz
Power Consumption:	80 watts



Three Encryption Modes are supported:

1. Select Encrypted Mode: In this mode, specified PIDs (up to 250) are encrypted. All other PIDs are passed from input to output unchanged.
2. Select Clear Mode: In this mode, specified PIDs (up to 250) are output in the clear. All other PIDs (except for the null PID) are encrypted.
3. Bypass Mode: In this mode, which can be used for tracking down system problems, all PIDs are passed through in the clear regardless of the list of selected PIDs. The PID list is preserved when this mode is selected so that it can be restored when one of the other modes is chosen during normal operation.

Digisat International Inc.
4195 W. New Haven Ave., Suite 15
Melbourne, FL 32904
USA
+1-321-676-5250
Email: sales@digisat.org
http://www.digisat.org