

Key-A-Minute™

Stand alone, 1 RU, highly secure, real time, Apache NginX Linux® Based, Rotating or Dynamic Key Server Designed to serve fresh AES-128 or DAES-128 encrypted keys once a minute via IP or other links to protect high value media from hackers. We provide an easy to use AES ciphering interface that can be adapted for multiple devices operating across public or private IP connections. Runs on an AES encrypted HP DL360 server with dual redundant power supplies. Comes with compatible client modules for your middleware or mobile device.



Features

- DAES-128 Encryption based on AES 128
- Fully automated 32 bit encryption and decryption
- Continuous Key Generation
- Encryption and Decryption are done in real time with minimal added latency
- Encryption process allows each packet to be individually encrypted
- Keys are generated with following parameters: Time Stamp Key, Media Object ID, Session Key, P In
- Supports any kind of IP content delivery device that supports reasonable calculation ability
- Key-a-Minute Server that contains master key can be locked up and the application runs in an encrypted eco system
- Communication with the system is done over a secure SSL API using HTTP REST requests with security based on username and password, certificates, or source IP address
- Remote management via HTTP
- Supports H.264 streams and replicated
- Configs can be saved
- Comes with client decryption app for your STB or mobile device

Applications

- Protecting IPTV systems from misuse

Overview

Digital Rights Management (DRM) is a necessary part of content distribution. It is mandated by content owners to control the use and modification of copyrighted material that was created with the expectation of a reasonable return on their investment. Each major "studio" creates their own requirements although major studios in the USA have banded together to create uniform DRM requirements. In the USA there are federal laws via DMCA laws.

AES is a data encryption standard established by the National Institute of Standards and Technology. It has been adopted by the U.S. government. It can be used for Top Secret information since it has been approved by the NSA. Many branded encryption platforms are based on AES-128, including ours which is known as DAES-128.

This product is a server that provides ever-changing DAES-128 "keys" to the end user devices.



Computer Modules, Inc.

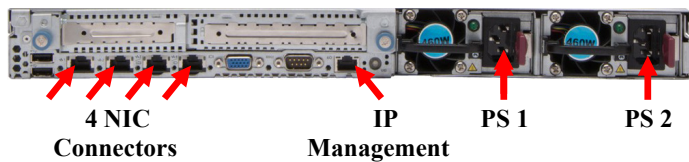
11409 West Bernardo Court

San Diego, CA 92127

Tel: 858-613-1818 Fax: 858-613-1815

www.dveo.com

Inputs/Outputs



Sample of GUIs – Coming Soon

Specifications

Encryption

Streams format:	IP-encapsulated MPEG-2 transport streams
Content Encryption:	128 bit AES or 128 bits DAES
Stream Encryption:	Selectable from 1-100%
Key Mutation Rate:	Up to every 2 seconds – Operator selectable per stream
Capacity:	50 to 100 channels per server
"Trick Play"/ DVR Indexing:	Single machine or distributed load balanced cluster, auto-failover support

Decryption

Decryption:	Includes client decryption app for operator's STB or mobile device
-------------	--







Administration

GUI:	Java based
SNMP:	SNMP v1, v2c, v3

CPU and Operating System

CPU:	Intel® Xeon® Quad Core
OS:	Ubuntu®

Physical & Power

Size – 1 RU high (W x D x H):	16.78 x 27.25 x 1.7 inches 42.62 x 69.22 x 4.32 cms
Voltage:	AC 120/230V, 50/60 Hz
Operating Temperature:	10°C to 35°C (50°F to 95°F)
Non-operating Temperature:	-40°C to 70°C (40°F to 158°F)
Operating Humidity:	10% to 90% relative humidity, non-condensing
Non-operating Humidity:	5% to 95% relative humidity, non-condensing
Weight:	17.92 lb (39.5 kg)
Conformities:	UL, BSMI, CSA, FCC, CE, RoHS      

Ordering Information

Key-A-Minute



Computer Modules, Inc.

11409 West Bernardo Court

San Diego, CA 92127

Tel: 858-613-1818 Fax: 858-613-1815

www.dveo.com