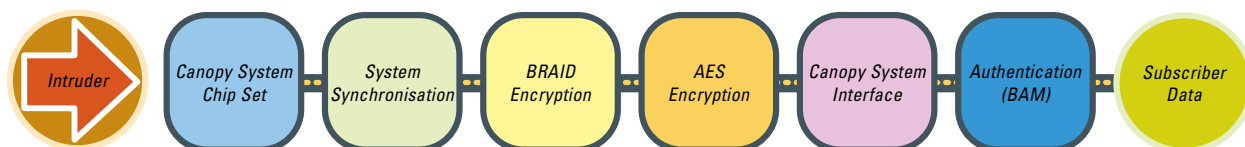


AES Product Portfolio

Motorola Canopy™ Wireless Broadband



Canopy System Security Architecture

Providing Subscribers with the Highest Level of Security

Today's security concerns have affected the way we live and work. Communications security needs to be impenetrable and simple to manage. Motorola Canopy™ wireless broadband systems can be enhanced with Advanced Encryption Standard (AES) to provide the required level of security demanded by many advanced users today. Entities ranging from financial institutions, public safety organisations, healthcare facilities, and larger businesses require the highest level of security available to ensure their data is safe.

Canopy System Security

AES is just one of the successive layers of security including hardware, software, interfaces, encryption, signal synchronisation and user authentication specifically designed into Canopy system communications. Motorola's 75 years of experience in wireless communication provides the highest level of security while also making the system reliable and accessible to authorised users.

- Exclusive Chip Set - The Canopy system's exclusive chip sets are a Motorola design and are not commonly available, reducing access to experience with embedded algorithms.
- System Synchronisation - The Canopy system's unique synchronisation technique provides higher security than 802.11 alternatives by requiring precise synchronisation from all modules in the network.
- BRAID Encryption - The AES key is encrypted by Motorola's 128-bit Telecommunications Industry Association (TIA) standard BRAID algorithm making it more secure than others in the market.
- AES Encryption - There are approximately: 3.4×10^{38} possible unique 128-bit keys protecting communication.

- Canopy System Interface - The Canopy system has a unique interface which is not published.
- Authentication - Canopy modules are authenticated when they are registered by the system. This function is controlled by the Canopy Bandwidth and Authentication Manager (BAM).

Note: If a machine could try 2^{55} keys per second, then it would take approximately 149 trillion years to crack a 128-bit AES key. For perspective, the universe is considered to be less than 20 billion years old.*

AES Module Benefits

The Canopy AES module adds 128-bit encryption that provides a higher level of security than filtering, Wired Equivalent protocol (WEP), Secure Sockets Layer (SSL) or Transport Layer Security (TLS). By deploying Canopy AES modules at strategic points in the network, operators can tailor the level of security to meet specific customer requirements.

- The National Institute of Standards and Technology (NIST) endorses AES encryption as the latest, most secure standard for communications.
- The Canopy system is the first to market in making AES encryption available for deployment. As a result, Canopy system service providers are the first to offer AES encryption to government and financial institutions where it is required.

Availability

AES is available on all Canopy products and may be ordered now.

Note: Canopy modules with AES Encryption are for distribution only in countries approved by the U.S. Commerce Department.

* <http://csrc.nist.gov/CryptoToolkit/aes/>



For more information about how the Canopy system can extend your network and services, provide competitive advantage and outstanding ROI, call 001-800-795-1530 internationally or visit us at www.motorola.com/canopy

Motorola Ltd, Europe Middle East Africa, Jays Close, Viabes Industrial Estate, BASINGSTOKE, Hampshire RG22 4PD, UK

MOTOROLA and the Stylized M Logo are registered in the U.S. Patent and Trademark Office. All other product or service names are the property of their registered owners. © Motorola, Inc. 2005. AES.SS-RE (07/05)

