

Product Brief

SecureMedia - Encryptonite™

“Transparently securing the world’s media”

For media organizations seeking a secure, reliable and high-speed encryption solution for their streaming media and premium broadband content, SecureMedia offers Encryptonite. Designed to secure your valuable data and create a transparent end-user experience, Encryptonite is the industry’s only complete end-to-end solution for protecting media from the point of origin all the way to the consumer.

With Encryptonite, media remains secure at every step of the distribution process – with no diminished functionality. Encryptonite offers real-time decryption, fast-forward and rewind for streaming and downloaded content, transportability to external devices such as MP3 players and set-top boxes, high reliability and a low cost. Now your organization can securely meet the instant delivery expectations that end-users have come to expect from traditional audio and video entertainment.

Unique product benefits:

- Uses a trusted and highly secure algorithm to provide extreme levels of security in broadband media applications
- Uniquely encrypts each data packet via a single master key and an indexed packet key, eliminating bandwidth-intensive overhead and providing unprecedented security
- Achieves the high execution speeds required for broadband audio and video delivery
- Protects media assets throughout the entire distribution chain, from source to point of rendering to end-user experience
- Transparent security makes Encryptonite user-friendly and maintains latency-free support for common VCR-style modes of operation such as rewind, fast-forward and search
- Can easily accommodate lost or out-of-sequence packets in real-time streaming situations
- Flexible implementation allows Encryptonite technology to be used in software and hardware applications
- Ideal for a wide range of applications including servers, PCs, set-top boxes, mobile players and Internet appliances
- Scalable from distributed caches and storage devices to millions of PC and non-PC users
- Implements with very little design overhead via a small software and/or hardware footprint
- Able to readily support alternative encryption techniques



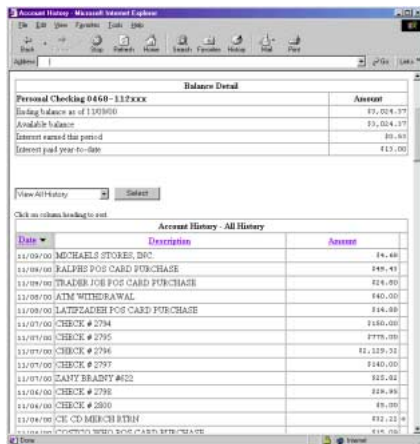
The Challenges of Encrypting Media

Protecting audio and video media presents serious compute intensive challenges that are not addressed with traditional encryption technology. The traditional on-line encryption model was designed to accommodate small amounts of data typically exchanged in a transactional manner. For example, credit card information, on-line banking and secure forms represent some of the more common types of secure data transfer. The amount of data involved in these encrypted transactions is small, which makes encryption performance less important. In addition, the order in which the packets of data arrive is also less critical, as messages are usually stored and viewed in a leisurely manner.

In the audio and video media world, files tend to be very large – often multiple megabytes more. Securely transferring such large files requires more compute power because the amount of data involved in the encryption and decryption process is larger by many orders of magnitude. Encryption challenges are further increased by the streaming requirement of many media files. As content is being viewed in a stream, that media must be decrypted, displayed and re-encrypted prior to displaying the next segment of video or audio. This high bandwidth and processor-intensive routine can significantly deter the end-user experience; a situation further complicated by fast-forwarding or rewinding content. With traditional encryption methods, the entire file must be processed through the encryption cycle from the beginning to move to other locations within the file. The result is a slow, linear process that diminishes the consumer experience. These challenges necessitate a new way to handle video and audio encryption.



Because of their large file size and the challenges of decrypting streaming media, audio and video files present unique encryption challenges



Traditional web based encryption was intended for transaction models such as on-line banking and electronic commerce

Media Encryption Requirements

There are a number of reasonable requirements that are necessary to maintain a user-friendly, yet secure, end-user media experience. A secure media transmission:

- should not impact the playback quality of audio or video (i.e., packets in streaming applications must arrive on time)
- must maintain an entertainment-level experience – users should be able to fast-forward or rewind (trick play) content with no impact on performance
- should be extendable from PCs to set-top boxes, MP3 players or other mobile devices and still remain secure
- must be reliable and highly available – it should not hang or crash the user's PC system
- needs a low cost of implementation – this allows more content creators to readily present their media on-line

Encryption 101 – The Advantages and Key Systems

The need to securely transmit media is more important than ever. Past developments within the recording industry make securing audio files a priority and it will not be long before video faces similar threats. The encouraging news is that audio and video media is essentially a massive grouping of binary code consisting of 0's and 1's. As with any number or series of numbers, formulas can be applied to the media resulting in scrambled and unrecognizable code.

With a proper encryption approach, the security taken for granted in the physical world can be achieved in the electronic world. With strong encryption and an accepted key exchange system, media can be readily transmitted over public networks (like the Internet) with little or no concern of rights infringement. A few legal benefits of secure encryption include:

Private Transmission: Media is protected against improper access or release.

Certified Communication: Only intended recipients can view or listen to files.

Data Integrity: Guarantees files are unaltered during transmission.

Authentication: Ensures that parties sending and receiving media are who they claim to be.

Media encryption creates a climate where piracy and fraud are eradicated, leading to a greater adoption and acceptance of Internet-based media delivery.

Public and Private Keys

A strong encryption system relies on a system known as *public key exchange*. With a public key system, what one key locks, only a matching key can unlock. In a public key system, public and private keys exist for both the user and the media file. Private keys are generated based on a true random number. From the private key, a public key is derived based on a one-way math function. The security level of the key is a function of the number of bits associated with the key. Based on existing technology, 600-bit public keys (or higher) make it virtually impossible to determine the associated private key. Public keys are made publicly available and are used to create a unique encryption scheme that only the private key holder can decrypt.

Encryptonite's Encryption Process – How It Works

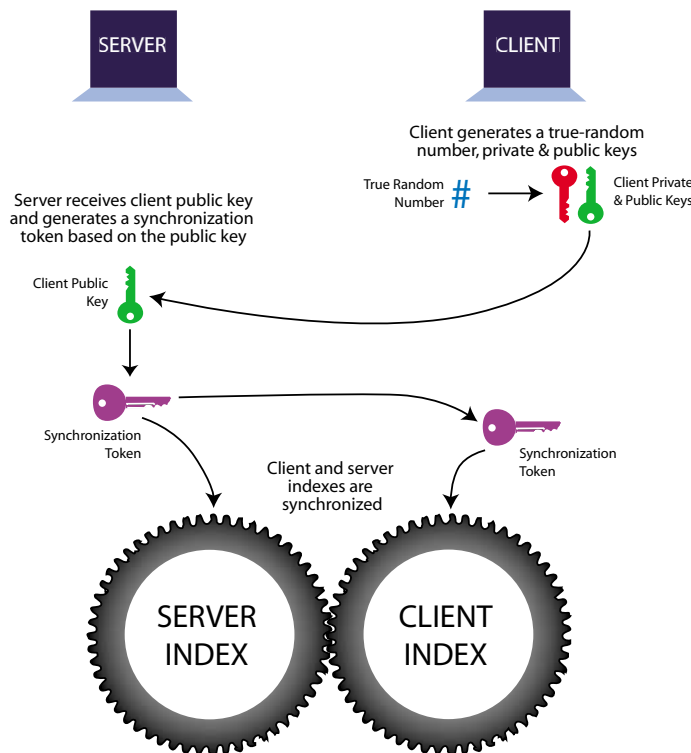
Encryptonite's encryption technique, known as Indexed Encryption™, is an internationally patented process that encrypts broadband media with no overhead, significantly enhancing performance. The core of Indexed Encryption is based on a combination of the time-tested and proven Diffie-Hellman cryptographic mathematics algorithm (see <http://www.apocalypse.org/pub/u/seven/diffie.html> for technical information) and breakthrough public key encryption technology developed by SecureMedia. Unlike alternatives, Indexed Encryption can accommodate lost, garbled or out-of-order packets.

Client / Server Initiation

With Encryptonite, both the server and the client contain the same set of trillions of unique packet keys contained in a virtual key chain known as a *shared index*. The first step in the initialization process occurs when the client generates a private encryption key based on a true random number generation process (see key synchronization illustration below). SecureMedia's patented random number generation process is based on the client's mouse movement patterns.

A one-way math formula is applied to the client's private key to derive the public key. Unique key sets are generated for each client session assuring that software keys are not compromised by remote hackers. The client's public key is passed to the server where it is used to create a synchronization token. The synchronization token determines which key in the index of keys will be used to begin the media encryption process. After the synchronization token is securely passed back to the client, the client index is synchronized with the server index. The client and the server are now ready to transmit secure packets of data.

Key Synchronization Illustration:



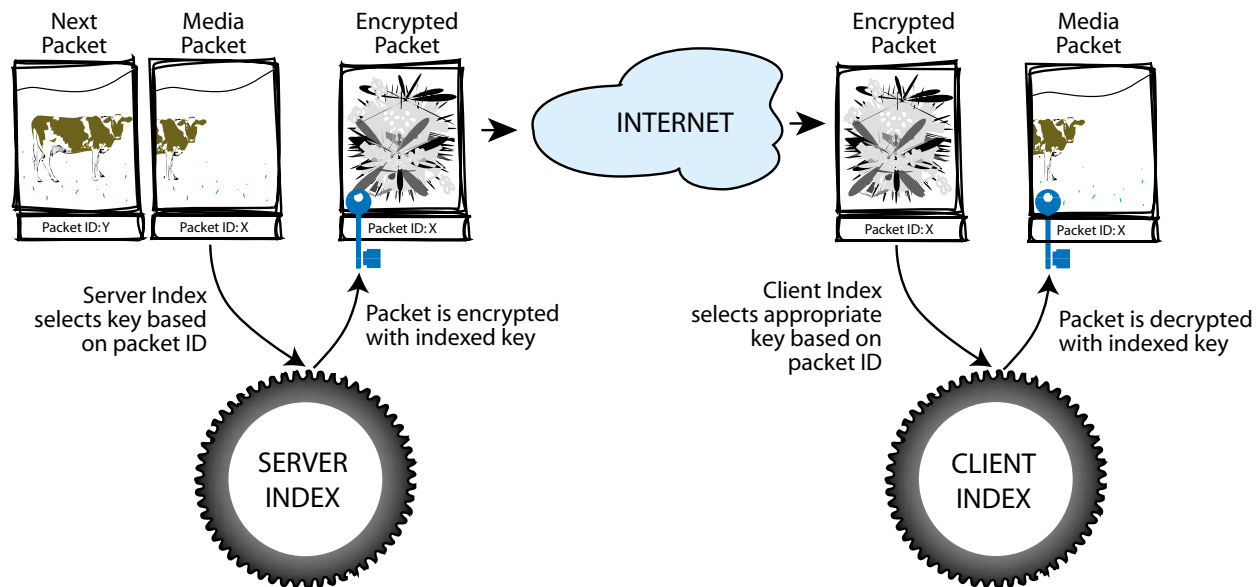
Secure Transmission of Media

Each media packet is encrypted based on the key indexing system. Prior to transmission, the client and server have been synchronized to a randomly selected key. The randomly selected key determines where in the universe of Encryptonite keys the encryption process should begin – a virtual home base. Using the unique packet ID associated with every packet, the Encryption Index will select a strong symmetric key that is derived from a mathematical relationship between the “home base” and the packet ID (see packet encryption illustration below). The Encryption Index is extremely secure because the “home base” is determined from a true random process on the client’s system and is securely transmitted to the server. Only the client and the server know which key is the starting key. Packet IDs by themselves can not determine the “home base” because they contain no information that points to the starting key.

Since the packets do not contain any keys at all, they can be streamed at significantly higher rates. In addition, packets do not need to be received in any particular order because packet encryption is not based on a packet’s relationship to other packets.

When the client receives an encrypted packet, the packet ID is used to determine which key should be used to decrypt the packet. All keys located within the Encryption Index are unique, random and not mathematically related. Each packet in a stream has its own unique encryption key. In the rare case that one packet is decrypted by a hacker, that person would only have access to a single packet. Hacking additional packets would be a time-consuming and difficult process. The likelihood of a successful hack is further complicated by extra-strong encryption keys from 612 bits to over 2200 bits.

Packet Encryption Illustration:



The outlined process is as follows:

1. Client and server key indexes are synchronized (see illustration on page 4).
2. Each packet of data is encrypted by keys that are determined based on a relationship between the starting key and the packet ID.
3. Each encrypted packet is sent to the client without key information.
4. The client receives the encrypted packet and decrypts it using the appropriate key as determined by the relationship between the packet ID and the starting key.
5. The packet of media is ready to be displayed.

The Encryptonite Advantage

Encryptonite combines the benefits of asymmetric public key cryptography (authentication, digital signatures, certificates and key management) with the speed of symmetric systems. The small code size of Encryptonite's underlying technology and its high performance approach make it the only encryption technology capable of wide-scale deployment in high-bandwidth Internet applications.

Technical Advantages of Indexed Encryption

Key Length: Indexed Encryption allows key lengths from 612 bits to more than 2200 bits without any negative impact on streaming performance.

Unique Encryption of Every Packet: If each packet is not encrypted with a separate key, the media is susceptible to parallel processing hacks by unauthorized parties. Because each packet has a unique key that is not related to the keys used in other packets in the media file, it is virtually impossible for a hacker to fully hack the entire media file.

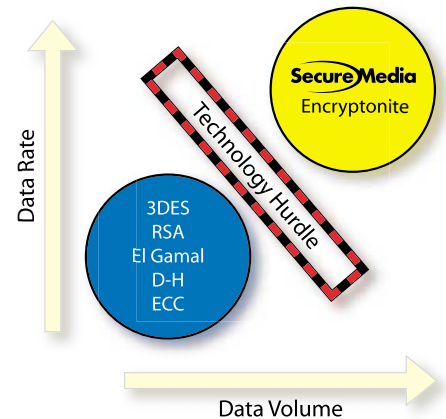
Based on Proven Diffie-Hellman Key Exchange: The Diffie-Hellman key exchange method is a well studied, respected and trusted form of key exchange. This key exchange system is highly secure because the problem of computing discrete logarithms in a finite field is a problem for which mathematicians know no shortcuts. In addition, in the streaming media marketplace, other newer techniques are not based on trusted cryptographic techniques.

Small Code Size: The Indexed Encryption code is much smaller than competing standards, making implementation more cost effective and allowing the code to be applied to silicon as well as software-based systems.

Why Alternative Approaches Don't Work with Media Files

Public Key Algorithms: Public key algorithms, such as Elliptic Curve and RSA, are useful for digital signatures and encrypting small amounts of data, such as information found in transaction-based procedures. For example, Encryptonite uses the Diffie-Hellman public key exchange to initiate sessions, which involves a simple exchange of random keys. The challenge with public key systems is more apparent when larger files, such as audio or video media, are encrypted. The processing power required to encrypt larger files with a public key system is problematic. In fact, public key algorithms were not designed for processing large amounts of data.

Block Ciphers: Block cipher algorithms uniquely encrypt each data packet. Common algorithms include DES, 3DES and AES. The two most common methods of block cipher encryption include cipher-feedback or multiple public key exchanges. With the cipher-feedback method, each packet in a media file is encrypted based on its mathematical relationship to the previous packet. The cipher-feedback model has inherent performance problems and the file security can be compromised by a hacker decoding a single packet and thus unlocking the entire file. The multiple public key exchange method presents serious performance issues and lacks scalability. If each packet must pass a unique key between the client and the server and the key is transmitted along with the packet, performance can be greatly reduced.



Encryptonite breaks technology barriers that others can not approach by securely transmitting data at extreme rates and accommodating large data volumes



Business Benefits of Encryptonite

Encryptonite is the only system that securely and reliably transmits high-speed streaming media. A number of key benefits include extreme performance, unprecedented security, an excellent user experience and integration with existing systems.

Extreme Performance

Encryptonite encrypts media on-the-fly as it is delivered from a web server to a user's media player. The extreme performance of Encryptonite allows content developers to securely present premium content at exceptional quality levels. This is uniquely achieved because keys never actually interact with data – meaning they are not embedded into packets. Removing the keys from the data stream reduces performance overhead and speeds transmission. This enables extreme encryption speeds – up to 20 Mbits per second. In contrast, DVD-quality performance is displayed at 5 Mbits per second.

Unprecedented Security

Encryptonite's underlying Indexed Encryption is based on the trusted Diffie-Hellman key exchange. Also known as the Diffie-Hellman problem, the cryptographic method is directly related to the difficulty of solving the discrete log problem over large finite fields. Encryptonite cannot effectively be cracked using distributed processing – the most common method used by hackers. The security level of Encryptonite is determined by the bit size of the encryption keys used, which are 612 bits or higher. Encryptonite's Indexed Encryption further increases packet security by disassociating keys from the encryption of other packets. This means that a packet key can not be derived from the encryption of previous packet. In addition, Encryptonite has also been analyzed by world-class cryptographers who have issued positive reports on the integrity of the technology.

Excellent User Experience

A positive user experience is a critical test of a successful encryption system. The user expectation with digital media is very high – excellent audio quality; crisp, clear pictures; uninterrupted performance and flexible file navigation. In order to deliver secure DVD-quality audio and video, an encryption system must achieve high levels of performance and allow for delivery anomalies. Encryptonite is the first and only system that achieves the performance required for DVD-quality media streaming and allows full file navigation. With Encryptonite, the decryption process is fully transparent to the user and he or she can fast-forward or rewind files with no latency issues. Encryptonite also takes the user experience one step further by enabling secure files to be extended from the PC to portable players and set-top boxes.

Integration

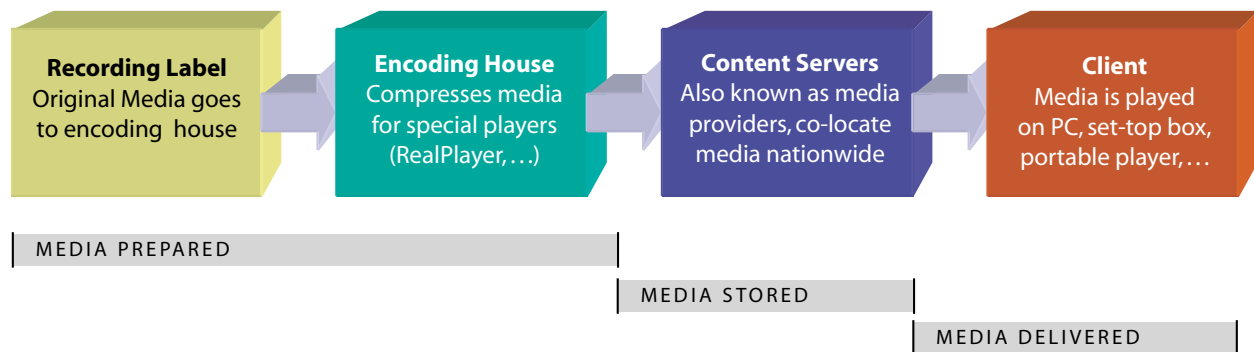
Encryptonite was designed to easily integrate with existing media delivery, management and control systems. Whether you're looking for a server-based encryption solution, an embedded solution or an encryption solution to integrate with design rights management systems, Encryptonite can and will accommodate your needs. Additionally, Encryptonite is content format independent, supporting RealSystem G2, RealAudio/Video/Flash/Pix, MP3, MPEG and others.

Encryptonite – A Total End-to-End Solution

The Encryptonite solution is like a highly mobile armored truck for digital media. Regardless of the location of the media – where it's prepared, where it's stored or where it's delivered – Encryptonite can ensure efficient and secure media delivery. Encryptonite lets labels encrypt their media in-house or with a trusted encoding house to increase security. With the Encryptonite system, media is secure at all stages of the distribution cycle. In traditional systems, unencrypted media is delivered to content servers where it's encrypted on the fly as it's transmitted to clients. The assumption with this method is that data is secure from theft or piracy prior to its delivery to content servers or after the media has been delivered to the client. Encryptonite offers a complete end-to-end solution that allows media to be encrypted at the source and delivered securely through all the distribution channels.

Encryptonite pre-encrypts media at the point of encoding all the way to point of rendering where the digital information is transformed into audio and video. This ensures that media sent over a distributed network to edge storage servers is secure. Additionally, as media is delivered to devices, the media is always passed in an encrypted state – it's never in the clear. Furthermore, when the player is ready to play the content, the decryption key is sent only at the exact time it's needed, thus the key is also never left in the clear.

Encryptonite's End-to-End Encryption Illustration:



Markets for Encryptonite

The applications for the Encryptonite solution are endless and include:

- Pay-per-view music, movies, video
- Private, access-controlled web-casting
- Secure videoconferencing
- Internal or external briefings, sales presentations, IPO road shows
- Remote training and communications
- Medical/pharmaceutical content
- Distance learning and education
- ISPs – secure remote hosting
- Secure music and video delivery, SDMI

Encryptonite – The Embedded Option

Due to its small code size, Encryptonite can be implemented in silicon at a cost-to-performance basis that delivers an order of magnitude better price performance than other encryption systems. Encryptonite is well-positioned for embedded deployment in consumer Internet appliances and devices such as MP3 players, set-top boxes, game systems, PDAs, cell phones and DVD players. With Encryptonite's inexpensive and small form factor, devices can provide strong encryption capabilities at processing speeds of 160 Mbits per second in a design that consists of no more than 20,000 gates.



**Encryptonite's embedded solution
will help protect media at the
player and Internet appliance level**

With only 200 KB of code, VHDI (Verilog) modules, low power, a low gate count and low overhead, the embedded Encryptonite option will enable secure media transmissions to extend beyond the PC.

The Encryptonite software toolkit comes complete with source code, comprehensive documentation and sample applications. With the toolkit, developers can create powerful embedded security solutions.

Toolkit Platform Support

The Encryptonite toolkit is available for a variety of platforms including:

- ANSI standard C/C++ libraries for Windows 95/98/2000/NT, HP/UX, Sun Solaris (C only) and Linux
- JAVA (confirms to JAVA security interface)
- Delphi 3.0/4.0 VCL component for Windows 95/NT
- DLL and ActiveX
- ANSI standard C library for use in embedded systems
- SDMI version for SDMI-compliant devices and software

Also compiled and tested with:

- Visual C++
- Borland C++ Builder
- gnu/g++