Securence™

Protect your business with email storage and retrieval that is fast, safe and affordable

| Reports | Quarantine | Shadow | Archive | Mail Logs | Deferred | Users |

Securence includes ten years of Email Archiving as part of the base offering. Email Archiving ensures the secure, simple and affordable storage of all inbound, outbound and internal electronic correspondence. Archives are searched easily and swiftly.

Securence Archiving is Fast

Documents are incorporated into the archive quickly and searches produce results in a flash. Queries run fast. Securence can search massive data bases and produce results **in seconds** in most cases. You won't have to wait minutes for a search to be completed, and you won't need to initiate and juggle several queries simultaneously to make up for up for slow processing time.

Securence Archiving is Advanced and Flexible

It's easy to setup and use **Exchange journaling** for internal email recording and storage, and to manage the complete archiving process. Securence supports your own internal email retention policy and facilitates compliance with federal and industry regulations. This provides you with:

- A proactive data loss prevention strategy
- Up-to-date auditing preparedness
- Documentation to fulfill legal requirements and hedge against litigation risk
- Support for your compliance initiatives for Sarbanes Oxley, HIPPA, SEC rules and other government regulations
- Data for use in Bates stamping

Indexing

Securence performs **full text indexing** of email messages and attachments from all Microsoft Office applications, PDFs and many more.

Search Capabilities

Advanced full text search and retrieval is simple and easy to use. All the options are there. Search by a date or a range of dates, by sender or recipient, by ID or IP address, for and through attachments, and by keyword in the subject line, message body or attachment.

Save your searches and rerun them at any given time to capture the unique results at the moment. Narrow your search results be adding additional criteria.

Secure Transport and Storage of internal and external messages. Storage is tamper-proof and read-only, keeping your messages protected in their original state. Securence **dual commit message capture** stores two copies of every message. If desired, messages can be stored at additional locations.

Encryption

As part of the archiving process, messages are encrypted and transported securely via TLS (also called SSL). Securence applies the best of AES-256 and RSA 4096 encryption methods to provide an encryption solution that is robust and fast.

AES-256 doubles the scrambling iterations involved in key generation in what is commonly regarded as robust under the 128-bit version, and is considered the "gold standard" among the top level security-conscious. Securence Archiving also complies with the FIPS (Federal Information Processing Standards) 140 requirements for cryptography modules.

When Securence encrypts a message for archiving, a unique, randomly generated AES- 256 secret key is used. AES is much faster than RSA and using it to handle large bodies of content keeps the process moving efficiently and smoothly.

Next, RSA is used to generate a public-private key pair which becomes a permanent part of the domain. The public key is then applied to encrypt the AES secret key.
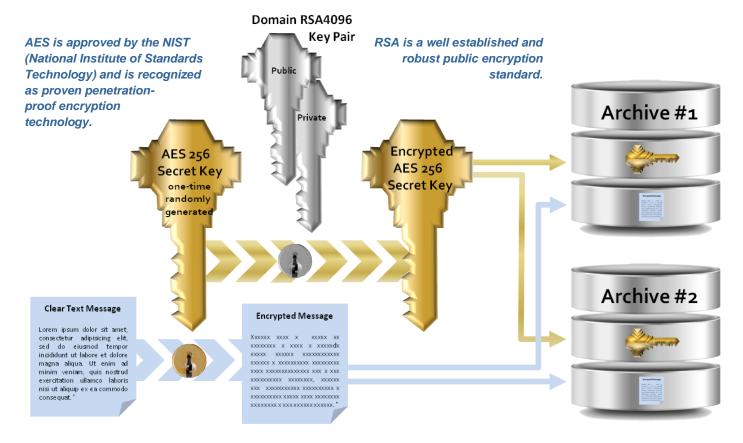
Next, the encrypted message is archived and stored in two separate locations. Similarly, the encrypted AES key is stored in the Securence private key escrow, also in two locations.

To retrieve encrypted messages from archive, a user logs on to his unique portal on the Securence site. His identity is authenticated and his private key, provisioned from the Securence private key escrow service, then decrypts his AES secret key, which then decrypts his email messages.

Advanced, Dependable Disaster Recovery

Add another layer of Securence to your Archiving strategy.
- Messages are stored in dual, secure off-site locations
- Records and stores emails in near real time as opposed to point-in-time backups
- Always running and not at risk to common hardware failures

AES is approved by the NIST (National Institute of Standards Technology) and is recognized as proven penetration-proof encryption technology.

RSA is a well established and robust public encryption standard.

Domain RSA4096 Key Pair

Public / Private

AES 256 Secret Key one-time randomly generated

Encrypted AES 256 Secret Key

Clear Text Message

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat."

Encrypted Message

Xxxxxx xxxx x xxxxx xx xxxxxxxx x xxxx x xxxxxdx xxxxx xxxxxx xxxxxxxxxxxx xxxxxx x xxxxxxxxxx xxxxxxxxx xxxx xxxxxxxxxxxxxx xxx x xxx xxxxxxxxxx xxxxxxxx, xxxxxx xxx xxxxxxxxxx xxxxxxxxxx x xxxxxxxxxx xxxxx xxxx xxxxxxxx xxxxxxxx x xxxxxxxxxxxxx xxxxxx."

Archive #1

Archive #2

Securence™ Archiving Encryption *Each message is encrypted with a unique AES key for each recipient.*