

Enabling Information Lifecycle Management Today

A White Paper on Adding the Power of ILM to Tiered Archive Storage

© 2005 Nexsan Technologies Inc.

All Rights Reserved.

Published by

Nexsan Technologies Inc.

21700 Oxnard Street, Suite 1850

Woodland Hills, CA 91367

USA

www.nexsan.com

Publication date: April 22, 2005.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage and retrieval system, without prior permission in writing from Nexsan Technologies Inc.

The information presented in this white paper represents the views of Nexsan Technologies Inc. (Nexsan Technologies) The information was prepared and reviewed for accuracy. However, Nexsan Technologies cannot guarantee that there are no errors or omissions. Nexsan Technologies makes no warranties, express or implied in this document.

Many of the comments and examples are related to the laws of the U.S., the United Kingdom and Canada as of the date of publication. The laws, regulations and jurisprudence in the area of compliance storage are constantly changing. Readers should review the current laws of their country, with their legal council, before making any decisions.

Nexsan Technologies and Assureon are trademarks of Nexsan Technologies Inc.

This paper describes areas of functionality that may not be available in all versions of Assureon, or on all OEM platforms.

About Nexsan Technologies

Nexsan Technologies (Nexsan Technologies) is a software technology company. The company does research and development in the area of long term digital file retention, management, verification, disposition and cryptology. The company currently licenses its software technology and services to computer storage vendors. Storage vendors that are licensees of the Nexsan Technologies technology can deliver solutions that meet the growing compliance regulations addressing electronic documents in the United States, European Union, and Canada.

Information about the current products, services and the company can be found at nexsan.com.

Table of Contents

About Nexsan Technologies 2

Table of Contents..... 3

The Challenges of Information Lifecycle Management 4

Regulations, Corporate Governance & Electronic Discovery..... 4

The Role of ILM in Meeting the Challenges 5

The Assureon Solution – Conquering the Toughest Challenges 6

Assureon Solution Architecture..... 7

Information Lifecycle Management powered by Assureon 9

Create 10

Classify..... 11

Place 12

Identify..... 13

Protect..... 15

Archive 18

Access..... 19

Expire 22

Summary..... 25

The Challenges of Information Lifecycle Management

Regulations, Corporate Governance & Electronic Discovery

Information Lifecycle Management (ILM) for electronically stored files is a challenge for most organizations.

“With so much business done today electronically, organizations facing a lawsuit, investigation, or an audit should expect that they will have to find and produce electronic information as part of the discovery process”¹

Digital storage is growing at an unprecedented rate and the conditions under which electronic information must be maintained and eventually deleted is becoming increasingly sophisticated. Recent deception and mismanagement of business practices in well known companies sent shockwaves through many industries. Government investigations, criminal suits and expensive regulatory fines, illustrated that there were flaws in the systems used to preserve and authenticate the corporate transactions and records for many of these companies.

New compliance regulations and renewed interest in existing laws have prompted businesses to change and tighten their internal controls. Implementing specific industry measures to meet regulations or establishing good corporate governance practices has become a priority.

Also the focus on electronic discovery in recent court cases, such as Enron/Andersen, clearly points out the flaws in record management systems used to preserve and authenticate corporate information. The courts expect all businesses to preserve and produce electronic evidence. There is no immunity.

¹ KCI Research, March 2005

Costs involving electronic discovery are high, and can lead to bankruptcy. Businesses will be required to:

- Pay large fines or face other heavy sanctions if they fail to produce the required information in a timely manner
- Absorb the expense of researching all their business records
- Prove the authenticity of their records
- Provide audit trails to demonstrate the trustworthiness of their employees, the processes, and the systems that are used for the preservation, retention and disposition of business records.

The Role of ILM in Meeting the Challenges

Worldwide, there are over 20,000 regulations² affecting the process by which records must be created, stored, accessed, maintained, and retained. These regulations specify the need for a business to properly monitor and manage the entire life cycle of their company's records. Business policies, processes, practices and systems can be audited to demonstrate compliance with the law.

The preservation, retention and disposition of electronic records will be costly if a company does not have a good ILM plan in place.

ILM is not new. The practice of ILM has been around since the paper filing cabinet. Today, with so much business done electronically, ILM practices from the past have evolved to include the electronic equivalent of filing cabinets: disk, tape, and optical storage devices.

ILM has become so important to the computer storage industry that the Storage Network Industry Association (SNIA) established an ILM initiative. The initiative provides a forum for the storage industry to promote industry collaboration. In the following paragraph, SNIA provides a definition of ILM that incorporates electronic document management for storage solutions:

² SNIA SMI-S: A Standard For Managing Storage, 2004.

“Information Lifecycle Management: the policies, processes, practices, services and tools used to align the business value of information with the most appropriate and cost effective infrastructure from the time information is created through its final disposition. Information is aligned with business requirements through management policies and service levels associated with applications, metadata, and data.”³

The key concepts in the definition are: the “alignment of business values with the most appropriate and cost effective infrastructure” and the “service levels associated with applications, metadata, and data.” Although these concepts are not new, it is their application to ILM that has created a new paradigm for the storage industry to embrace.

The Nexsan Technologies Assureon ILM solution is based on years of research and development. It is a new generation of storage management software, designed with the new paradigm in mind. Assureon is storage hardware independent, and as such will help companies to successfully achieve the alignment of their business values with the most appropriate IT infrastructure. Assureon is also modular and very scalable, so it matches the service levels associated with applications, metadata, and data.

The Assureon Solution – Conquering the Toughest Challenges

Assureon is a solution that enables organizations to use their best practice rules and at the same time fulfill their compliance requirements. Assureon is not tied to a specific storage infrastructure (disk, tape or optical storage) and provides the most cost-effective means for managing the lifecycle of information in a tiered storage infrastructure.

Assureon assists in the management of business information from its creation to final disposition and can be used by any business, regardless of its size. The compliance capabilities of Assureon are configurable, so the alignment of the value of the information can be set to the specific retention and disposition policies of individual regulations, such as SEC 17a-4, HIPAA, CFR 21 part 11 FDA, Sarbanes-Oxley, Privacy Regulations, and so on.

³ SNIA ILM Definition and Scope, An ILM Framework, July 28, 2004.

Assureon Solution Architecture

Assureon is a software application composed of two main components:

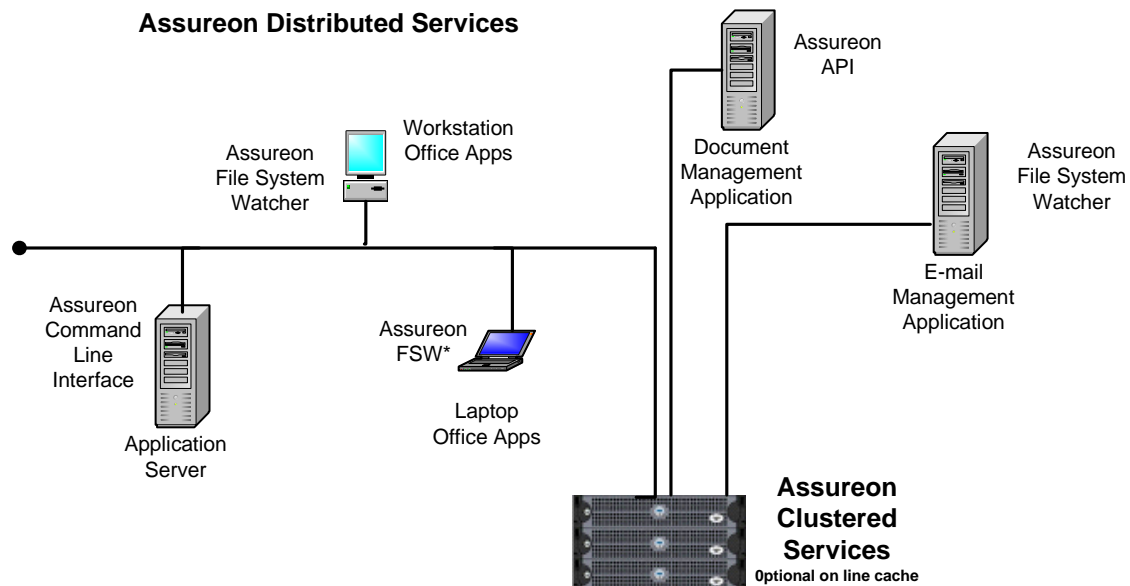
- Assureon Distributed Services (ADS), which capture and classify digital content
- Assureon Clustered Services (ACS), which store, manage, secure, provide access to, and handle the disposition of digital content.

Distributed Services are implemented through one of three software clients:

- Assureon File System Watcher (FSW)
- Assureon Application Programming Interface (API)
- Assureon Batch Interface.

The software clients are installed throughout an existing infrastructure on application servers, workstations or notebooks, and capture electronic content continuously, even from notebooks that are disconnected from the network.

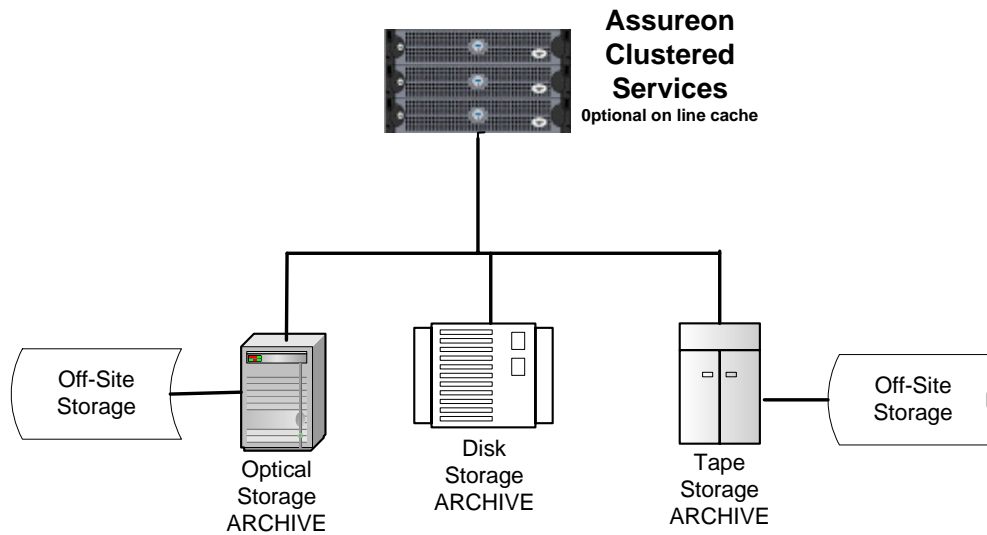
Figure 1: Assureon Distributed Services



Assureon Clustered Services are pre-installed on industry standard Intel based appliances running Microsoft Windows .NET Server. This allows for scalability and fault tolerance. Assureon can be configured for a disk, tape or optical storage subsystem or a multi-tiered storage infrastructure as illustrated in Figure 2.

Figure 2: Assureon in a Tiered Storage Infrastructure

Assureon in a Tiered Storage Infrastructure



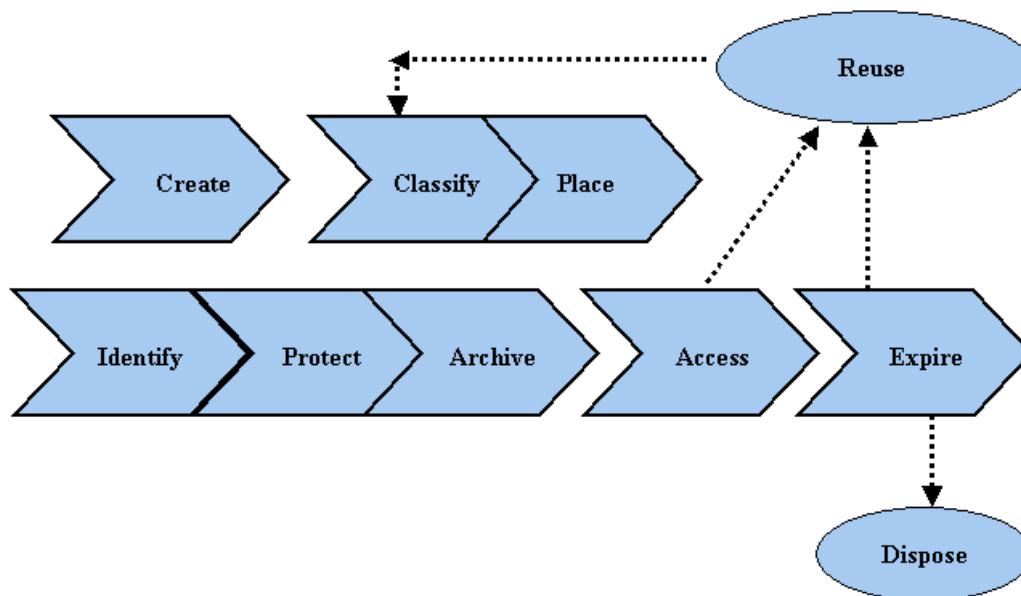
In the next section, the SNIA ILM reference model is presented and compared to the Assureon ILM solution.

Information Lifecycle Management powered by Assureon

SNIA not only provided the storage industry with a definition of ILM, it also defined an ILM reference model. The model defines the essential stages of the ILM process and has the following seven stages: Create, Classify, Place, Protect, Archive, Access and Expire.⁴ See Figure 3 for an overview.

When SNIA proposed the model, Content Addressable Storage (CAS) was new, and not taken into consideration. CAS uniquely identifies every file under its management and maintains a single instance store of each file. Nexsan Technologies sees CAS as core technology for any ILM solution, and has added another stage, called Identify, to the model. The identify stage can significantly reduce the cost of long-term archive storage. Table 1 associates the essential requirements of ILM to Assureon capabilities.

Figure 3: Stages and Functions of ILM



⁴ SNIA Strategic Profile: Information Lifecycle Management, A Vision for the Future, 2004.

Table 1: Stages of ILM and Assureon Capabilities

ILM Stage	Assureon Capability
Create	Captures structured and unstructured information
Classify	Applies or generates retention policies
Place	Moves the file to storage locations based on policies
Identify	Produces unique identifier based on content using Assureon Content Addressable Storage (CAS) technology
Protect	Secures the file through its lifecycle
Archive	Manages long term storage of the data on all media
Access	Provides secure access to information
Expire	Manages the disposition of the information regardless of location and media

The ILM reference model is a good starting point for any company wanting to compare the features and benefits of different ILM solutions. The following sections describe the functionality of Assureon in more detail at each of the stages.

Create

Most electronic documents start their lifecycles as drafts. Their content is expected to change. At some point, the content becomes fixed and protected, and an event is triggered to create a reference copy of the electronic file. The trigger can be completely transparent to the content creator or a deliberate action that needs to be made, such as saving a file to a particular directory.

Fixed content is created from many general office applications, such as Word, Excel, Lotus Notes, Power Point, and Outlook. These applications produce both electronic and paper documents, such as contracts, emails, proposals, presentations, and so on. Unless special measures are taken by the authors to preserve the fixed content, the content can be easily changed by anyone who has access to the files.

Fixed content is also generated by specialized applications that produce a variety of electronic file types, such as simple electronic transaction reports, medical images, ERM/computer output, financial reports, check images, snapshots of web sites, photographic images, video surveillance images, call center recordings, and engineering drawings.

The problem with most applications used to generate content is that they are not ILM savvy. The content author must use some other application or tool to preserve and establish file attributes for retention and disposition. So in addition to creating content, the author needs to classify it. Not so in the Assureon model.

Classify

An organization will create policies for the classification of fixed content information using criteria such as content value and regulatory requirements. How an enterprise implements and manages these policies will vary. If a business uses a Document Content Management (DCM) application, it may perform classification within the application; DCM applications provide the capability to place certain classifications on the information and file types.

Many larger organizations use DCM applications to organize and classify their fixed content. DCM can be implemented at the enterprise level, but is typically implemented at the departmental level, and is not generally available to all content creators.

In the small to medium business (SMB) market, DCM application implementations are not common, as the cost of ownership is prohibitive.

Email archiving applications are also becoming increasingly popular for organizations to help manage and control the ever increasing volume of emails. Like DCM applications, email archiving applications may also be used to classify emails and their attachments.

Assureon automates classifications and can also be integrated with existing DCM and email management applications. If a third-party application generates the file classifications, Assureon can be configured to use the same classifications to manage the files.

Assureon Distributed Services are designed to capture, and classify, electronic files from original sources. More importantly, ADS are easy to install and manage, and when configured for an individual content creator, automates all the capture and classification processes for every file created, no matter the application used. These capabilities are available through any of the Assureon Distributed Services, including the Assureon File System Watcher.

Assureon File System Watcher

Assureon's FSW is a capture and classification program for electronic content that uses a policy based rules engine. The rules engine organizes the retention and disposition policies for every content creator, and automates the classification process.

The FSW is configured to monitor a directory, or group of directories. Policies can be set up per directory, so that any changes made to a file in a monitored directory will trigger selection and processing rules. Processing rules determine whether the file is deleted or kept in the original location, its storage location, who can access the stored file, how long the file is kept, and so on. The FSW can be completely transparent to the content creator.

The FSW is one of three services provided by ADS. The other two services of ADS, the ADS Batch Interface and the Application Programming Interface (API), are more specialized. They are intended for businesses who want to customize the integration, such as, place large volumes of existing documents under management at one time and use Assureon with third-party applications or who want to use special features that are only accessible via an API.

After a document is classified, the FSW also processes rules for the ILM Place stage.

Place

In the ILM model, Place determines the storage location of a file. With Assureon, an ADS service, like the FSW, moves a file from its original location to archival storage, based on configurable policies. Policies related to how the original file is handled include:

- Delete original file
- Keep original file in its location
- Replace original file with a shortcut
- Keep original file in its location based on certain rules, such as time since last accessed, size, number of times accessed, and so on.

By default, the file is stored in a minimum of two locations.

The power behind the ADS is the rules engine, which automates the implementation of ILM policies. Policies can be easily customized to fit the needs of individual content creators. Assureon makes it easy for content creators to classify and place their valuable fixed content in secure archive storage while transparently working in the background.

The next stage in the ILM process is the Identify stage, which is an Nexsan Technologies addition to the SNIA model. This stage was added because Assureon uses Content Addressable Storage (CAS) to store electronic documents.

Identify

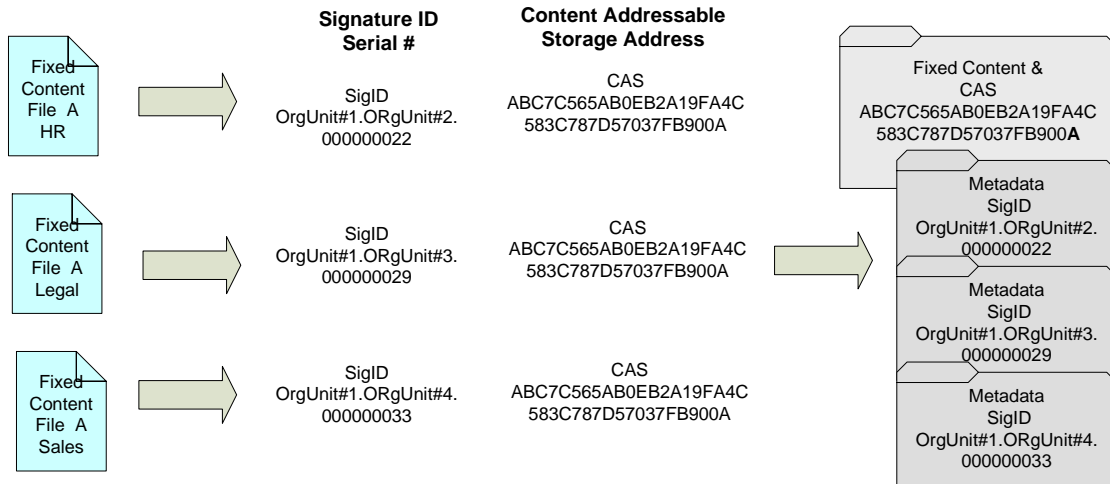
The long-term retention and management of information requires that an organization's files be assigned a unique identifier that is independent of the application used to create them, a particular file system or specific storage device.

Assureon employs file serialization and Content Addressable Storage (CAS) technologies to accomplish this. A significant benefit of CAS is true single instance storage whereby only one copy of a file is kept. Analysts concur this could potentially reduce the amount of files stored by 20 to 60 percent.

The identity challenge occurs when multiple instances of the same file are being stored with different life cycles. For example, the HR and Finance department may be storing the exact same file, but for compliance reasons each department has different retention policies associated with the file; the Finance department has a three year retention period while HR has a five year period. Assureon addresses this challenge by using two types of identification: sequential serial numbers for the instance of the file, and a unique CAS address for the file itself, as illustrated in Figure 4.

Figure 4: CAS, Single Instance Store & Serialization

Content Addressable, Serialization & Single Instance Store



Serial Number Identification

Assureon assigns a unique serial number for every storage request or instance of a file which is called the Signature Identifier or SigId. The serial number is sequential and has a multi-level structure which can be configured to identify client, business division, project name, and so on. For example, a company could have two divisions, using a common business model based on projects, departments and employees. Assureon lets you leverage existing structures by allowing you to manage stored files using a similar structure

The serial number is also secured through the use of digital time stamping and digital signature technologies. Assureon uses these processes to generate a rich metadata structure, which addresses auditing requirements as found in compliance regulations.

CAS Address

CAS identifies files based on their content by using cryptographic hashing technology. Using a content based storage address instead of the file name enables single instance store, insuring that only one copy of the original file is kept.

Recent research⁵, confirming Nexsan Technologies' own findings, has shown that a single cryptographic hashing process, such as MD5, can produce the same CAS identity for two different files. If this "hash collision" were to occur where single instance store is being used, it would result in one of the files being discarded and lost, forever. Reliable single instance store requires fail-safe CAS technology. Assureon's unique dual cryptographic hashing process provides that assurance.

To guarantee that a single instance of the content is placed under management, two cryptographic hash functions (MD5 and SHA-1) are used to generate a unique file identifier (UFID). Assureon uses these standard hashing algorithms to generate digital fingerprints (128 and 160-bit respectively) of the original file. By using multiple hash functions and other attributes of the file content, Assureon guarantees that there is a single UFID for each instance of file content in the system. The UFID provides the CAS address that is used to store and locate the archived file. The address can also be used to store files across multiple folders and physical devices, allowing for exceptional scalability and load sharing.

The next stage in the ILM process is the Protect or preservation stage. Once a file is classified, placed, and uniquely identified, Assureon will properly protect the file for its lifetime.

Protect

ILM systems must protect files and preserve the integrity of files under their management. One model for protecting and preserving the integrity of files is to store them and then limit access to the archive.

Another model allows users to have access to the archives, but to encrypt the files so that only authorized users, using encryption keys, can read the content of the files. This model also audits access, and produces reports to prove that the integrity of the ILM system is not being compromised. Assureon uses this model.

⁵ Cnet News.com "Crypto researchers abuzz over flaws" Aug 17,2004

Assureon protects and preserves files under its management using several cryptographic technologies. When a file is placed under management, Assureon adds tamper-protection to both the file content and the associated file information and policies (the metadata). These protection mechanisms ensure that archived files can be retained securely.

Security based on cryptographic technologies offer the best form of security. Assureon uses several cryptographic technologies, each of which is described in the following sections.

File Encryption

Assureon optionally encrypts the file content before writing it to the archive storage system. This provides at-rest data protection, ensuring that information cannot leak from the storage system. By encrypting all content, an organization is conforming to the confidentiality requirements of current regulations (such as HIPAA, California SB 1386, Privacy Regulations, and so on.).

Assureon uses the AES (Advanced Encryption Standard) algorithm to encrypt file contents. Each file is encrypted using a unique 256-bit AES key. Encryption is selective and policy based, allowing for user, department, project or organizational encryption rules. Assureon incorporates a redundant key manager, which provides secure and redundant key storage. Advanced functionality includes crypto shredding; the ability to destroy encrypted file objects that are stored offline or on WORM media.

File Integrity

A digital file has integrity if it can be demonstrated that its contents have not been altered. An ILM system must be able to prove the integrity of any retrieved file. The standard approach is to retain a hash of the file, which can be checked over the lifetime of the information. Assureon improves on this approach by maintaining the following integrity checks:

- The MD5 and SHA-1 hash values of the original file are saved in the metadata.
- The metadata files are digitally signed with the precise date and time.
- A catalog listing the metadata files, their digital signature information and past catalogs is created, digitally signed and placed under management. This process ensures that any tampering with the signed metadata is detected.
- Optionally, the signed catalogs can be stored with a trusted third party in order to create a legal record of all files stored.

Assureon constantly validates the integrity of all files under its management.

Cryptographic hints are included with all stored objects, allowing for fast verification without the need to decrypt the files to validate their authenticity. Files that fail the verification process are deemed to be corrupt and are replaced with an integral version of the file. This ongoing process ensures that digital files stored with Assureon retain their integrity, no matter how long the files are kept in storage.

File Authenticity

Authenticity is the proof of origin of the file – who created it, when was it created, how it was created, and so on. Assureon maintains this proof in the metadata by retaining the file information associated with the file (collected by the FSW). Assureon also establishes its own authentication data by:

- Serializing all files in order to track whether files are missing (a SEC requirement); and
- Time stamping the metadata. This time stamp is generated by a local Time Stamp Provider (TSP) with its own time source in accordance with industry and regulatory standards.

Assureon ILM will help an organization establish trust in their fixed content and reference data. Assureon also supports the use of a Trusted Third Party (TTP) to establish trust in the Assureon system. Assureon periodically generates a catalog that is submitted to the TTP for notarization (digital signature, time stamping, and storage). This process allows for independent verification of the entire ILM system.

Integrity and Authenticity Audit

Audit is a critical component of an information security system – providing verification of these protection mechanisms. Assureon generates standard activity and access logs that can be incorporated into the organization’s accounting systems (enabling reactive audit). Assureon also supports proactive audits by using audit agents. These agent processes continually audit an organization’s Assureon ILM system and operate at multiple levels:

- Integrity of assets – checking the archived files (against their digital signatures). This satisfies the SEC requirement for automatic testing of the quality of the data recording.
- Authenticity of assets – checking the metadata against the content
- Independent third-party audit of the catalog.

A good proactive business strategy for protecting any valuable company asset involves planning, processes, and execution. If a company is asked to do electronic discovery in order to defend against a lawsuit, the court will expect the company to prove that the security umbrella that protects the business records is tamper-proof. Using Assureon to protect and preserve the company’s archived business records is a good proactive strategy, and greatly simplifies the electronic discovery process. Assureon security is tamper-proof, and ensures authenticity of every record that it manages.

The next stage in the ILM process is the Archive stage, which deals with storage.

Archive

The SNIA definition of ILM states that tools need “to align the business value of information with the most appropriate and cost effective infrastructure from the time information is created through its final disposition”. Nexsan Technologies designed Assureon to be storage agnostic, so it supports all forms of archive storage technology, aligning it perfectly with the SNIA definition of ILM.

Hierarchical storage management (HSM) systems migrate files from primary storage to archive storage, based on their inactivity. The lack or delay in writing the files to permanent storage media, is not appropriate for compliance reasons. Nor is the lack of proper safeguards and audit controls, which could bring the integrity of the files into question. Assureon takes a very different approach.

Assureon writes the files under its management to two or more permanent storage media devices, and optionally, to an online cache. Safeguards, such as file encryption, and audit trails, ensure the integrity of the files. Then, based on established policies, Assureon will delete the file from its original location as the file transitions from an active to an inactive state. The automated removal of inactive files from fast, expensive storage media, provides significant cost savings.

Assureon allows a company to store files on any combination of WORM (Write Once Read Many) disk, tape or optical disk devices. For example, a company may want to have its primary archive on a WORM disk (for fast access) and a copy of the archive on (slower) optical disk. This flexibility allows for additional cost savings.

Many CFOs and CIOs view the Archive stage as a huge IT investment. IT managers can use Assureon to show that company files, including archived files, are being properly managed and stored on the most appropriate type of storage.

The next stage in the ILM process is the Access stage, where controlled access to archived files is defined.

Access

Providing access to fixed content and reference data is an important consideration in the design of long-term retention systems. Reference data is a valuable company asset and as such, it needs to be made readily available to different groups within an organization.

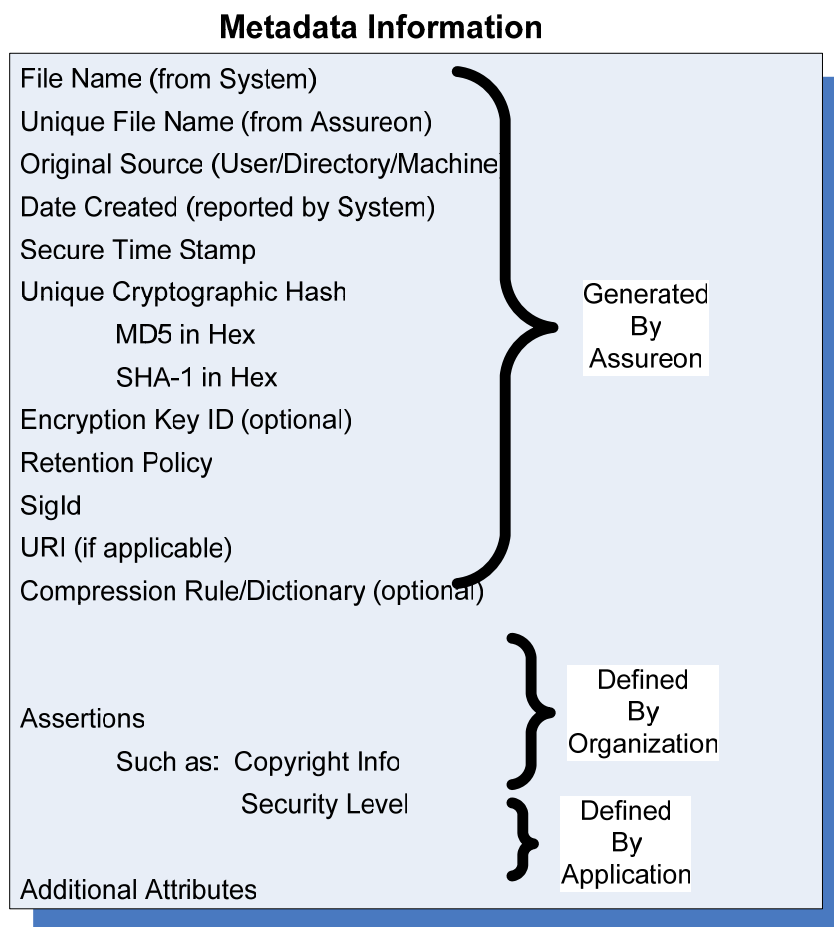
When access is required, it must be easy and immediate. An ILM system must guarantee that archived information can be located and retrieved when needed.

Assureon Metadata

Assureon keeps three levels of information on every file under its management:

- The first level contains file information generated by Assureon. This level has, for example, name, time stamp, encryption, and policy information.
- The second level is defined by the organization, and can include classification categories, privacy information, security statements, and so on.
- The third level is defined by any third-party application, such as an email or document management application.

Figure 5: File Metadata Stored by Assureon



Assureon also stores file metadata in an SQL database, which may be searched using the Assureon search feature. Locating a file, or any other information embedded in the metadata, is fast and convenient.

Reliable Storage and Access

Files under Assureon management are written multiple times to multiple archive storage systems, depending on the organization's requirements. The Assureon protection mechanisms associated with each archived file guarantees that an authentic and integral copy of the original file can be retrieved.

Assureon is implemented as a web service – files can be retrieved though an intranet or Internet connection. This advanced architecture ensures an organization of accessibility to their electronic documents.

Policy Based Access Control

Controlled access is especially important for compliance reasons, where privacy laws protect the confidentiality of the reference data. Controlled access also needs to be administratively easy to manage, and change over time.

The Assureon system acts as the Policy Enforcement Point (PEP) that controls whether or not a specific user is allowed to access the decrypted content. This provides an organization with “breach law” protection – restricting information access to authorized users. Access control policies for the file are added to the metadata during the Protect phase and checked during the Access phase. The Assureon PEP also allows the organization to track access to files by application or user (a HIPAA requirement).

Assureon Access Control

Assureon access control has three components:

- Authentication verifies that a user is who they say they are:
- Assureon uses Microsoft's Authentication System
- Assureon optionally uses security certificates (Smart Cards)
- Authorization determines that the client has the appropriate permissions to access the resources they are requesting. Authorization is given to an authenticated client by policies established within Assureon and then published into Microsoft's Active Directory.
- Audit logs that can be used to account for any and all access to managed information.

The final stage in the ILM process is the Expire stage. No meaningful discussion on ILM and the preservation of information can be conducted without discussing the expiration and disposition of electronic files. Once again, Assureon has some very powerful ILM capabilities at this stage of the lifecycle.

Expire

At the end of a retention period, a file becomes inaccessible to users and becomes a candidate for disposition. The file needs to be deleted in all locations or have its retention period extended. Given that there is always a chance that a regulation could change, or a court case could request that the life of a document be extended, Assureon does not automatically delete an expired file. Instead, it allows file disposition to be suspended or for the extension of an individual file's retention period, with user access enabled or disabled.

Most compliance regulations require the protection of information for a fixed retention period. To comply with these regulations, Assureon will not allow any files under its management to have their retention periods shortened and provide tamper protected retention periods, guaranteeing that the life of a document cannot be shortened by accident or willful intention.

At this point, it is worth mentioning that a file can be accessed and reused at any point during its lifecycle. As soon as the file is modified, it becomes a new file, and if placed under Assureon management, is given a new retention period.

Disposition of All Files

As previously mentioned, at the end of a retention period a file becomes a candidate for disposition. To securely dispose of expired files, the Assureon system provides a list of disposition candidates for the system administrator to approve for disposition. The list can be generated daily, weekly or monthly, depending on the needs of the organization.

The disposition process itself runs on a daily basis at a configurable time and can be cancelled.

The disposition process begins with a detailed audit of all files approved for disposition. If the audit is successful, and no tampering or integrity violations have been found, the system begins the process of scrubbing the selected files. After the files have been securely removed from the accessible storage devices, a crypto key scrubbing process is scheduled. Crypto key scrubbing is an optional step used to destroy remotely archived files or files that are stored on hardware based WORM storage media, tape, CD or DVD.

Prior to Assureon, it was virtually impossible for an organization to be assured that all copies of electronic files had been disposed of at the end of their retention periods. This was due to technologies and policies in place. For example:

- Many companies use WORM (Write Once Read Many) optical or tape for their long term archiving. Once a file is written to media, it is impossible to delete unless the entire optical disk or tape is destroyed. Disposition is not practical because files on the same media will have different retention periods.
- The computer industry has developed backup processes to ensure files are not lost due to computer failure or disaster. Multiple copies of files are stored on backup media, very often offsite. At the time of disposition, it is next to impossible to retrieve and delete all copies of an expired file.

The traditional technologies and process problems have legal and compliance implications. Certain regulations require that all copies of digital files be destroyed at a certain point in time. Not disposing of electronic files at the end of their retention period exposes organizations to needless risk, through the electronic discovery process.

Assureon's technology and processes allow files to be securely and completely disposed of from any media. Once a file or its key has been scrubbed, the file becomes nothing more than a random series of bits; it cannot be accessed, read or reconstituted.

Scrubbing

Assureon follows a very specific procedure to assure proper scrubbing of data and encryption keys, meeting Department of Defense requirements.

- Pass one: File is open & Assureon writes binary 1s to every bit in the file.
- Pass two: File is flushed to disk and closed.
- Pass three: File is reopened and Assureon writes binary 0s to every bit in the file.
- Pass four: File is flushed to disk and closed.
- Pass five: File is opened, and Assureon writes alternate 1s and 0s to every bit.
- Pass six: File is flushed to disk and closed.
- Pass seven: File is then deleted.

The encryption technique not only allows for the disposition of files, it allows for the secure storage of files at rest. Only authorized personnel can access files under Assureon management. Also, security is not compromised if unauthorized access to offline media occurs, which recently occurred to Bank of America's back up tapes.⁶ The Assureon disposition processes are simple to manage, and ensure that all files, whether on or off line, are disposed of at the proper time. The Assureon disposition processes also work for WORM, and non-WORM formats of disk, tape and optical devices.

⁶ Bank of America Loses a Million Customer Records" Robert Lemos, CNET News.com, Feb 25,2005

Summary

Given that ILM has been mandated worldwide by over 20,000 regulations, implementing an ILM solution is the right business decision. When you consider that the costs of electronic discovery can bankrupt a company, investing in an ILM solution, especially an affordable one like Assureon, makes perfect sense.

Assureon offers a cost effective way of implementing an ILM strategy for today's compliance challenges. Assureon can be tailored for small, medium or large businesses and is easy to implement and maintain over time. It can also be integrated into existing enterprise third-party DCM system and email archiving systems.

Assureon was designed by Nexsan Technologies to adapt with the changes in compliance regulations, and new DCM, ILM and Storage technologies. In a world of constant change, one constant is Nexsan Technologies' dedication to meeting the needs of its customers.