Data Management Forum

Securing Email: Best Practices in ILM Security

A DMF ILMI Best Practices White Paper

October 1, 2004

SNIA
STORAGE NETWORKING INDUSTRY ASSOCIATION

Copyright 2004 SNIA Data Management Forum

Author:
Clement Kent, CTO, Kasten Chase Applied Research Ltd.
Member DMF ILMI Technical Liaison Group
Secretary IEEE P1619 Security in Storage Working Group

Table of Contents

© 2004 Storage Networking Industry Association

1. Introduction

The SNIA definition for ILM [1]:

> 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.

This definition includes how data is to be secured within the IT infrastructure. This white paper is intended to provide best practices in data security for email over its whole life cycle.

This paper is one in a series of white papers produced by the SNIA Data Management Forum's ILM Initiative specifically for IT Administrators as the intended audience. It is written with the intent of providing IT Administrators with usable, application-specific, guidelines on deploying ILM solutions using today's technologies.

Each white paper defines best practices for a specific dimension of ILM solutions. In this paper, the topic is data security for email.

1.1. Purpose and Scope

This white paper describes Security best practices for major email systems such as Microsoft Exchange, Lotus Domino, and SendMail in the context of Information Lifecycle Management (ILM). Three other papers deal with related issues in ILM for email – Best Practices for Protection, Best Practices for Archiving, and Compliance Overview (see References [3-5]).

Many best practices for security must be understood, planned, and implemented in the context of best practices from Protection, Archiving, and Compliance. To avoid reinventing the wheel, we will refer to the other white papers in this set for definitions and explanations of many of these concepts.

Other SNIA Best Practices White Papers cover general Storage Networking Security [9] and special topics in Object Storage [10].

1.1.1. Email Application Scope

This paper focuses on widely used email applications such as Microsoft Exchange and Lotus Domino, and SendMail.

1.1.2. SAN, NAS, DAS environments

The primary focus of this article is on email implemented in storage networking environments. Most recommendations are independent of storage type. Email Servers using DAS for primary storage are nonetheless often backed up using network methods, so this will be discussed from the security viewpoint as well.

© 2004 Storage Networking Industry Association

1.1.3. Data Security versus Data Protection

For the purpose of this document, data security and data protection will be regarded as distinct.

- Data Protection will mean protection of data against loss, and protection of the organization using the data against downtime due to data loss or corruption
- Data Security will mean security in all senses *other* than data protection as defined above. This includes ensuring the confidentiality, authenticity, and integrity of email data through the life cycle.

1.2. Considerations for Security

As in the rest of ILM best practices, security is based upon policies. Policies in turn are designed to meet fundamental business goals, such as maintaining confidentiality, integrity, and availability of business email information. Many of these policies and goals are well understood in the context of live, production email systems (for a full description of these, see [7, 12]). However, over the full ILM cycle security policies and goals may change, and aligning them with data protection policies and methods is important. In particular, multiple different policies will govern data in different data store, for instance in an Operational Recovery(OR) backup and in a Compliance Archive. For example, an account may have full access to the backup but none to the archive, or vice versa (see discussion also in [4,5]).

A few examples of the kinds of issues that may differ between production management of email data and full ILM management of security will help clarify what's at stake:

A) Archiving and Backup for data protection and efficiency
B) Archiving for Compliance

In case A, a company we'll call XYZ Widgets (XYZ-W) has been rolling out a combination of backup methods and an email Archiving tool. XYZ-W has done this to meet cost containment and QOS goals. The archiving tool helped reduce the size of online email databases, which in turn significantly reduced the backup window for email and improved the IS department's confidence that recovery of lost messages or corrupted databases would meet quality of service goals such as RTO and RPO (see SNIA Dictionary for definitions). The archived messages are held on lower-cost storage devices so the email system's average storage charge-back costs have been reduced. However, a recent company security audit revealed that the email archive is not as strongly defended as the production email database, raising the possibility this system might be more easily targeted by hackers or disgruntled employees. The storage team has been asked to provide new access policies to the archive and put them into practice.

In case B, a multinational brokerage firm, ABC Dealers (ABC-D) has been studying the impact of U.S. compliance laws and regulations such as Sarbanes-Oxley and SEC rules. Based on this study a company goal of retaining all ABC-D broker communications in a separate long-term archive has been stated. The archive must support legal discovery searches under defined conditions, as ABC-D is currently defending itself against 2 lawsuits alleging wrongdoing by its brokers. ABC-D has purchased a Discovery, Archive, Retrieval, and Compliance (DARC) product. The current company email backups do not lend themselves to such searches so a project has been initiated to transfer the existing Exchange 5.5 and 2000 backups for the

© 2004 Storage Networking Industry Association

brokerage department into the DARC product. The project is called "Putting Email into the DARC" and the project team is in the dark about how to apply the Exchange 5.5 and 2000 Exchange Server KMS (Key Management Server) security features to the DARC archive.

These two examples show that companies often adopt different tools for managing the later phases of the Exchange information lifecycle, based on different business goals for using this information.

1.2.1. Policies over Time

Policies must be sensitive to the different roles and responsibilities of people and processes in the organization when information is at different stages in the life cycle. Technical measures for Data Protection, Archiving, and Compliance will introduce new means and modes of storing information, and must be accompanied by security policies specifically adapted to these information environments.

Primary information security policies are those for the live or production copies of information. Secondary information security policies are those which apply to information in OR or DR backups, archives, and compliance databases. As mentioned before, very often completely different policies apply to OR or DR data from those applying to compliance data.

Secondary security policies will inherit some components from primary policies. An example would be the email archive at XYZ-Widgets Corp., where most of the access to archived messages is by the original recipients of the messages. In other cases, the people and processes allowed to see messages in ABC-Dealers' DARC database will be the indexing and discovery tool itself and the company legal and compliance staff. Original message recipients may have no rights to see their messages in the DARC database. In this case, secondary policies do not inherit any properties from the primary policies, and must in fact be completely separate.

A very important best practice in ILM Security is therefore to examine security policies carefully for each information type over its life cycle, and characterize how policies change over the cycle.

Best Practice:

- Classify each email data store at each stage of its life cycle
- Clearly indicate policies applying to non-operational data and how they differ from operational data policies

1.2.2. CIA: Confidentiality, Integrity, Availability

Security goals are often summarized by the easy-to-remember acronym "CIA": Confidentiality, Integrity, Availability. Confidentiality and Integrity are well understood in the storage industry, but the security officer's definition of Availability encompasses the restrictive meanings associated with Authentication, Authorization, and Access Control, in addition to the familiar data protection-based meaning of ensuring data is available when needed.

The several constituent parts of CIA are defined and enforced through metadata about people, information, and system components, and the application level security checks which attempt to match constraints defined in policies to security metadata. It is this security metadata, along with

© 2004 Storage Networking Industry Association

the appropriate policies, which ILM must manage along with the email data throughout the life cycle.

In the context of Exchange or Lotus mail, security metadata may exist in multiple forms:

- People: LDAP, Active Directory, Domino Directory or Notes ID entries, Exchange KMS entries, specific email Application permissions for administrators, delegates, and other,
- Information: message header fields (recipients, etc), security labels, additional security assertions in formats such as S/MIME [6], IRM "rights licenses" in the form of XrML [11], or Defense Messaging System MSP formats [8,13]
- Components: privileges, permissions, etc at the level of applications such as archives, as well as identity information for components (for example, authentication methods and credentials for devices in a storage network).

Information metadata is most tightly linked to or carried within the information data formats in the email application, while People and Component security metadata tends to be bound to objects not managed directly by the ILM system.

Important exceptions to this rule apply however when message or attachment formats such as S/MIME and IRM are impenetrable unless the enabling People security metadata is still accessible. For example, if IRM is used to limit viewing of a Microsoft Office document held as an attachment in a message to a list of people, then validating security information about one of that list of people will be required to view the attachment in an archive. Or, if S/MIME signing was used to provide authentication and non-repudiation of the identity of a message sender, then certificate information from Active Directory, Domino Directory, or another LDAP system will be required to confirm the signature during a legal investigation years later. Finally, if confidentiality of the message was achieved by S/MIME encryption of the message contents, an archive discovery and indexing system would require access to the private encryption key of one of the message's recipients, either at time of insertion of the message into the archive (archive stores clear text) or later (archives stores S/MIME or IRM format messages).

Another exception to the separation of People information from email application information is that Exchange allows (but does not require) personal security metadata such as certificates to be held in Contacts folders, while the Exchange 5.5. and 2000 KMS (Key Management System) is a predecessor and alternative to Active Directory for storing some of the same information. In these cases, the Exchange data managers must determine an ILM policy for this personal security data held within Exchange, as well as a recovery policy should this data need to be used in some later rebuild of a working Exchange system from backups and archives. Similarly, for Domino, administrators must ensure backups of Domino Directory and, in some cases, Notes ID files are subject to the ILM policies which apply to the email data.

In special environments such as government, additional security policies such as MLS (Multiple Level Security) will be enforced through systems such as MAC (Mandatory Access Control) based on security labels attached to messages in such formats as ESS-S/MIME v3 [13].

1.2.3. Synchronizing Protection and Security

In the previous section we looked at security attributes relating to CIA, especially in later life cycle stages such as archives. Data Protection (see [3]) of live production email systems is associated with another set of ILM Security best practices, most of which are focused on

© 2004 Storage Networking Industry Association

ensuring that the Data Protection environment maintains consistent views of email data and of related security systems, such as LDAP, Domino Directory, Active Directory, Exchange KMS, logs, and so forth.

The integration between Exchange and Active Directory is high. Exchange administrators are careful in migrating from Exchange 5.5 to Exchange 2000, to migrate security and user data from internal Exchange formats to external Active Directory formats.

In the example of ABC-Dealers above, the "Putting Email into the DARC" project leaders had to deal with such format conversions, because ABC-D had backups of Exchange systems of different ages and Exchange versions. Data Security best practices mean that data protection system for Exchange must protect:

- Active Directory forests,
- Exchange KMS if used,
- Windows Server 2003 Certificate Services if used,
- and/or any other LDAP or internal CA (Certificate Authority) system used

These must be retrievable at or near the same Recovery Point as the Exchange message stores and logs. If this system consistency can't be provided, operational problems with recovered Exchange systems may result, or security breaches are possible.

Similar comments apply to Domino when certificate information from an external LDAP system is used instead of the internal certificate stores supported by Domino Directory. Such mixed-directory systems are especially likely to be encountered in companies supporting a multiplicity of email system types.

Antivirus and Worm filtering and Content Filtering applications run in close conjunction with email Servers. Such filtering should be done before data replication and archiving. Feeds to Compliance archives (DARC systems) are often taken from email journals; it is essential to ensure that filtering happens before the journaling point, or that a duplicate filtering process is installed for archives. Otherwise, unfiltered content may contaminate backup and archive stores.

1.3. Security and the ILM Process

Building ILM into your systems is a process that begins with business goals definitions and data classification, and proceeds on to policy definition, implementation architecture and design, and finally implementation and operations management.

In many respects the best practices for processes for ILM security are identical to ILM process best practices and Security process best practices.

1.3.1. Building in Security at the Beginning

Both ILM and security start with definition of business goals. In the case of security, questions of the business value of the components of security should be addressed in this stage, including threat models. Threats alone can't determine security policies, however, since a large security threat to low value data may be less important than a minor security threat to business-critical data.

© 2004 Storage Networking Industry Association

Compliance and legal experts within the organization should provide input in the ILM planning stages, along with the CSO's security staff, to harmonize potentially conflicting legal, compliance, security, operational, and business goals.

1.3.2. Data Classification and Security Classification

Data classification by business value is an integral part of the ILM process. Data classification by security value should occur as part of the same data classification exercise. In government environments, security classifications may be externally dictated independent of data's business value. In commercial environments, the security value of data will be determined in part by legal and regulatory issues (violating HIPAA rules in a health care company would be very bad news, so customer personally identifiable health data must be strongly protected; for organizations doing business in California, State Law 1386 may mandate special protection for customer identity and credit data).

The output of the data business, security, and compliance classification exercise should result in a joint classification of each type of data from each perspective at each stage of the data's life cycle.

© 2004 Storage Networking Industry Association

2. Email Security over the Information Life Cycle

Security policies and best practices associated with each email application configuration, operational considerations and implications, disaster recovery, compliance archiving, all need to be defined for each information lifecycle stage for email.

2.1. Security and Storage Networking

A quote from the SNIA OSD group highlights some areas of storage network security which can be provided by the network components themselves or the fabric as a whole:

> "A complete and useful environment will:
> a) Authenticate application client identities,
> b) Test each requested operation against the environment's database of authorized transformations,
> c) Ensure that the integrity of each operation is not tampered with during transmission,
> d) Protect the privacy of data, access patterns and application clients,
> e) Identify the source of inappropriate activity, and
> f) Survive inappropriate activity with minimal degradation of service qualities." [10], sec. 4.4.4.1

If the fabric or network can provide authentication, test authorization, ensure transmission integrity, protect data privacy, and highlight and survive attacks, best practices in storage network operational security are being followed.

Applications such as email or email archiving products cannot be fully secure unless their storage network environment is secure.

At present, many products are being upgraded to provide more comprehensive fabric or network security system in the above sense.

Best Practices:

- Conduct a storage security assessment
- Build an action plan for using existing product security features more fully
- Identify additional security-enhancing products and plan their integration

A useful reference is the SNIA Storage Security Industry Forum (SSIF) Storage Networking Security Best Practices [9].

© 2004 Storage Networking Industry Association

2.2. Security and Backup & Recovery for operational systems

See our white paper [3] for more details on this topic.

As noted in section 1, security policies for the several types of later-stage email data stores must be carefully examined to match the policy to the ILM method and use of the data. Data stores meeting different ILM goals will have different policies.

Best Practices:

- Virus/Worm filters are used before data enters server email databases
- OR (Operational Recovery) copies of mail databases are made at least every 4 hours during peak message load periods to ensure infection-free database recovery copies are not too old
- Access Control for OR copies is equivalent to ACL for live mail databases
- DR copies of mail data should be synchronized with DR copies of security systems such as Active Directory, Domino Directory, or LDAP data.
- Where offline copies are made as part of OR or DR, physical security of the transport, storage, and retrieval of offline copies must be as high as the physical security of the main production data centers, unless data is encrypted before transport and storage
- Data copies that leave company custody should be protected against unauthorized use by policy-based combinations of physical security and digital security, such as encryption of media.
- If encryption is used to protect data copies, ensure encryption strength and mode meets company and government policies. For instance, some backup applications use DES encryption, which is being phased out by the U.S. government; the U.S. National Institue of Standards and Technology (NIST) has suggested use of Advanced Encryption Standard (AES) encryption to replace DES and other older methods.
- If encryption is used to protect data, all backup and archival policies which apply to data should have parallel policies applying to encryption keys, to ensure the keys are secure and protected to the same degree as the data.

© 2004 Storage Networking Industry Association

2.3. Security and Remote Replication

See our white paper [3] for more details on this topic.

Because DR sites and offsite media repositories are often less visible to operational staff, security policies protecting the DR data need special attention to ensure there is a mechanism for determining security policy compliance. Data is exposed in various ways

Best Practices:

- Physical security and access control at remote or DR sites must be as high as at primary data centers, unless other measures such as encryption are used to limit risks of confidentiality breaches. DR sites must be periodically inspected for compliance to security policies.
- When non-company staff operate equipment at DR sites, security vetting, training, and metadata (certificates, ACL, etc) should be defined by policy for non-employee DR staff.
- When data transmission methods from primary to remote sites are not fully under company control (e.g. 3rd party MAN or WAN links are used) a policy for protection of data in transit should specify whether digital methods such as data encryption must be used.
- Stored copies of email at DR sites or offsite repositories should be encrypted unless physical security of the repository or DR site meets company policies. See section 2.2 re encryption strengths and methods.

© 2004 Storage Networking Industry Association

2.4. Security and Email Archiving Systems

See our white paper [4] for more details on this topic.

In this section we distinguish between email archives, typically maintained for compliance reasons [5], and OR or DR copies. Special attention to differing access control policies for such compliance archives is required. Unless such policies are well thought out, the compliance archive can be a confidentiality risk to the corporation.

Best Practices:

- Security for e-mail archives should be as high as for live email databases. Policies should dictate who should have access to the archives and under what conditions.
- Security Policies for email archives should be jointly approved by the company's CSO and CPO (security and compliance staff must agree on these policies).
- Archives with limited user access should be in separate segments (zones, VLAN's, etc) of company networks.
- If the company's mail system contains confidentiality-protected messages (using S/MIME, IRM, etc) a system of ensuring secure access to the contents of such messages within the archive must be in place.
- As archives may be stored at different sites or in 3rd party repositories, data in such locations should be encrypted unless physical security meets policy goals at the remote sites. See section 2.2 re encryption strengths and methods.
- A central, searchable directory of all copies of data in the archive should be maintained, including backups of the archive system.

2.5. Secure Data Destruction

Mail will be retained for a planned lifetime governed by retention policies based on legal compliance needs. Companies will also ensure mail is removed from archives, and backup copies after retention periods to reduce liability.

Best Practices:

- A full directory or audit log of repositories or locations in which mail data resides should be maintained
- When mail data has passed its retention lifetime it should be removed from all locations in the above directory
- Removal of data should be complete, by means of physical media destruction, data wiping, or in the case of encrypted data, audited destruction of the encryption keys.

© 2004 Storage Networking Industry Association

3. Other Considerations For Securing Email Data

This section describes security best practices for email data over its lifetime other than those treated in section 2.

3.1. Tiers of Storage: Archive Solutions Security

The final store of most email data in companies governed by compliance laws will be non-operational archives, intended for long term storage, with write-once read-many (WORM) characteristics.

See our white paper [4] for more details on this topic.

3.1.1. Confidentiality and Access control

Because archives are managed by different people, must divulge their contents under different conditions, and are often not as visible to data center staff as operational systems, special attention needs to be given to confidentiality and access control policies, procedures, and protections.

See also section 2.4, above.

Best Practices:

- Policies should explicitly describe roles having access to archived mail data and the conditions of such access
- Technical methods such as encryption of archived data, access control based on archive roles, and physical and logical segregation of archive data from operational data should be used to prevent unauthorized access.

3.1.2. Audit trails on Access

Archives which may be used for legal purposes must be appropriately audited and logged. Failure to do so, especially for end-of-life data deletion, or data copy during refresh cycles, may reduce the legal value of the archive and open the company to non-compliance risks.

Best Practices:

- Policies should state whether read access to archives requires auditable records. If required, access methods should record in a secure audit log evidence of read access.
- Write access to archives should be prohibited except for initial data load operations (see data integrity below).
- Delete access must be policy based and audited in a secure log if so dictated by policy.

© 2004 Storage Networking Industry Association

3.1.3. Data Integrity

Proving that archived data is complete and unmodified is a primary business goal of the archive.

Best Practices:

- Archive systems must provide a set of physical or logical control preventing modification of archived data (such as WORM, Write-Once, Read Many).
- Prevention of modification must extend to all copies of archived data. For instance, if the primary store of a mail Archive is a disk system with WORM controls, but the data on the system is backed up to tape for offsite protection, other measures must be in place to assure integrity of the tape backups. Digital methods such as cryptographic signatures of archive data may be used when physical enforcement of WORM is not available.

3.1.4. Linkage to Media Refresh Cycles

At policy-based intervals data will be copied from older archive media to newer ones to ensure continued readability. Ensuring integrity under media refresh is required. (see 3.1.3)

Best Practices:

- Policies and procedures must govern media refresh cycles to ensure that data is neither omitted from the refreshed copies nor modified or added to.

© 2004 Storage Networking Industry Association

3.2. Interface with Security Systems

Best practices in long-term management of mail data require that security systems used with the mail systems be protected and controlled as much as the mail data itself. This section repeats some points made earlier, but here with the highlight on the interfaces to accessory security systems.

3.2.1. Directories (LDAP, Active Directory)

Stores of identity and authentication and cryptographic information such as LDAP, Domino Directory, and Active Directory servers, Certificate servers, and independent key stores are integral to secure functioning of email data systems such as Exchange or Lotus, and even to archives of email data.

Best Practices:

- Data Protection, Security, and Archival policies and procedures for email must cover protection, security, and long-term archive of associated security information, including certificates, signing public keys, encryption private keys, and LDAP, Domino Directory and Active directory databases.
- Email moved to an archive for long-term retention must retain the capability of authentication and decryption. This may be done by either (a) verifying and decrypting email on storage in the Archive, in which case signing and decryption keys do not need archival, or by (b) leaving email formats intact and ensuring signing and decryption keys are archived with equivalent lifetimes and retention methods to the archived email.

3.2.2. Physical Security in Archives

Physical security for some archival methods is endangered by the “out of sight, out of mind” phenomenon. When physical security for archival media is not as strong as for operational media, other compensating means such as encryption of the media should be used to prevent unauthorized disclosure of company data. See section 2.2 for more details

Best Practices:

- Physical security controls on access to archived material should be dictated by policy, based on the determined need for physical security of the data over its anticipated lifetime.
- All copies of archives, including tapes, spare disks, CDs, etc should be in the scope of the physical security policies. Off-site 3rd party media storage firms should provide evidence of compliance with security policies.
- Encryption of archived data may be used to substitute for stronger (and thus more expensive) forms of physical security. In such cases policies concerning encryption strength and method should be enforced (see section 2.2 for more details).

© 2004 Storage Networking Industry Association

3.2.3. Audit Controls

Logs and other sources of audit information are often a primary target of attackers who wish to modify digital data. Such logs are also one of the primary proofs of compliance with data retention regulations.

Best Practices:

- Audit logs of data movement by the ILM system(s) handling email are themselves secured and archived.
- Audit logs should be protected and secured as strongly as the underlying email data. In particular physical and digital protections of audit logs are required. Where possible audit logs should be under separate control from the systems they monitor.
- When policy so dictates, audit logs should show creation, read access to, media refresh of, and final deletion of long-term email data.

3.2.4. PKI and other key management systems

Most of the issues regarding PKI and key management systems are covered under 3.2.1, Directories, and are not repeated here.

Note that in the past PKI systems were focused on protecting short-term message traffic. Expiry of public keys is an integral part of PKI systems and is enforced by certificate expiry dates, certificate revocation lists, etc. However, when public keys and certificates have been used to provide authentication of sender identity or confidentiality of email messages, the long-term retention of email should be accompanied by long-term retention of public and private keys and certificates, even when these may have expired from active use.

Best Practices:

- PKI system data such as public and private keys and certificates must be protected as long as the underlying email data they apply to, and at security levels appropriate to the protection of highly secure material.

3.2.5. Anti-Virus and other Filters

Recognizing the time-lags between virus release in the digital environment and virus scanner updates to catch these viruses, a double layer of defense is desirable for long-term data.

Best Practices:

- Messages should be scanned by up to date virus/worm scanners before entry into operational email databases.
- Scanners should have virus definitions updated at least daily; if policies permit, on-demand push updates from antivirus vendors should be used to minimize update lag.
- Mail data being moved by ILM systems to near-line or archive stores should be re-scanned to catch viruses whose definitions were not available at time of system entry.
- Archive systems should support a quarantine for entries found to be infected and an audited re-archive of such entries with disinfected versions. Since archives will be WORM, this will require marking infected versions for early deletion.

© 2004 Storage Networking Industry Association

4. References

[1] SNIA Dictionary: http://www.snia.org/education/dictionary

[2] SNIA DMF ILM Best Practices White Paper: Securing Email: Best Practices in Security for ILM, SNIA Data Management Forum, October 2004

[3] SNIA DMF ILM Best Practices White Paper: Best Practices in Data Recovery for Email, SNIA Data Management Forum, October 2004

[4] SNIA DMF ILM Best Practices White Paper: Archiving and Tiered Storage for Email, , SNIA Data Management Forum, October 2004

[5] Managing Email for Compliance and Litigation Support - An Overview, SNIA Data Management Forum, October 2004

[6] Hoffman, P., Editor "Enhanced Security Services for S/MIME", RFC 2634, June 1999.

[7] Secure Messaging with Microsoft Exchange Server 2003, by Paul Robichaux. Microsoft Press, 2004.

[8] FIPS PUB 188: Standard Security Label for Information Transfer, U.S. Dept. of Commerce / National Institute of Standards and Technology, September 6, 1994.

[9] SSIF Storage Networking Security Best Practices. SNIA SSIF, July 2003. Editor: Arthur Edmonds. http://www.snia.org/apps/group_public/download.php/3008/SSIF%20Best%20Practices%202.6.03.pdf

[10] OSD SCSI Commands. ftp://ftp.t10.org/t10/drafts/osd/osd-r05.pdf

[11] XrML- The Digital Rights Language for Trusted Content and Services. www.xrml.org

[12] Lotus Notes and Domino R5.0 Security Infrastructure Revealed. Editor: Fiona Collins. http://publib-b.boulder.ibm.com/Redbooks.nsf/RedbookAbstracts/sg245341.html?OpenDocument

[13] "Secure Data Network System (SDNS) Message Security Protocol (MSP) 4.0", Specification SDN.701, Revision A, 1997-02-06.

© 2004 Storage Networking Industry Association

5. Available Products for These Solutions

The following DMF member companies have solutions that support one or more of the best practices defined in this white paper. The following URLs are provided for additional information.

COPAN Systems: http://www.copansys.com

COPAN Systems' Revolution 200T uses patent-pending Power Managed RAID™ and Disk Aerobics™ technologies to provide 224 TB of MAID storage in a single footprint with 2.4 TB/hour throughput. The Revolution 200T is ideal for backup/recovery and active archive applications offering the performance and reliability of disk, at the cost and scale of tape.

EMC²: **http://www.emc.com/products**

EMC products offer strong native security capabilities, supporting confidentiality, authentication and integrity mechanisms. Support for partner LDAP and anti-virus solutions enhance privilege management and content security. Combining EMC's Legato E-mail archiving solutions with EMC's Centera ensures the authenticity and integrity of mail for Microsoft Exchange, Lotus Notes and other fixed content records.

Kasten Chase: **http://www.kastenchase.com/**

Kasten Chase's Assurency™ SecureData storage security solution provides security and encryption for stored data throughout the data lifecycle. SecureData enables storage consolidation, streamlines data management and enhances regulatory compliance. SecureData's Lifecycle Key Management provides policy-based, audited key creation, protection and deletion, ensuring efficient data compartmentalization and assured data destruction.

Permabit: http://www.permabit.com/

Permabit's Permeon software enables companies to cost-effectively store archived electronic content, including email, for compliance and reference purposes. With secure replication, AES encryption, automatic media refresh, and WORM volume support, enterprises can easily implement industry best practices, and comply with even the most stringent government regulations for record retention.

© 2004 Storage Networking Industry Association

About the Author:

Clement Kent is Chief Technology Officer of Kasten Chase. He has over 25 years of experience in software engineering, including storage security, business intelligence, and semiconductor chip fab CIM (computer integrated manufacturing). At Kasten Chase, he has been responsible for leading development of SAN storage security products, participation on standards groups, and most importantly working with customers and partners on meeting future needs in storage security deriving from fields such as archiving, ILM, and SIS. Clement is currently a member of the SNIA DMF's ILM Initiative Technical Liaison Group and of the SNIA ILM Technical Workgroup. He is secretary of the IEEE Security in Storage Working Group which is developing the IEEE P1619 stored media encryption standard.

About the Data Management Forum:

The SNIA Data Management Forum is a cooperative initiative of Information Technology Professionals, Vendors, Integrators, and Service Providers formed to define, implement, qualify, and teach improved and reliable methods for the protection, retention, and lifecycle management of electronic data and information.

About the SNIA:

The Storage Networking Industry Association is a not-for-profit organisation made up of more than 300 companies and individuals worldwide spanning virtually the entire storage industry. SNIA members share a common goal: to set the pace of the industry by ensuring that storage networks become efficient, complete and trusted solutions across the IT community. To this end, the SNIA is uniquely committed to delivering standards, education and services that will propel open storage networking solutions into the broader market.

© 2004 Storage Networking Industry Association