
Defense Message System Way Ahead

Conclusions and Recommendations from the Industry Advisory Panel

March 1, 2000

REPORT DOCUMENTATION PAGE

Form Approved OMB No.
0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY) 01-03-2000	2. REPORT TYPE	3. DATES COVERED (FROM - TO) xx-xx-2000 to xx-xx-2000
---	----------------	--

4. TITLE AND SUBTITLE Defense Message System Way Ahead: Conclusions and Recommendations from the Industry Advisory Panel Unclassified	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS DoD Industry Advisory Panel XXXXX XXXXX, XXXXXXXX	8. PERFORMING ORGANIZATION REPORT NUMBER
--	--

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS DoD Industry Advisory Panel ,	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT A PUBLIC RELEASE ,
--

13. SUPPLEMENTARY NOTES

14. ABSTRACT The DoD Industry Advisory Panel was formed to update the DoD Messaging Advisory Panel Report of 1997 with emerging technology trends and to provide recommendations on the way ahead in view of commercial directions in the next 2 to 5 years. This report presents our findings and recommendations, as well as background materials and summaries in the Appendices.

15. SUBJECT TERMS IATAC Collection; defense message system

16. SECURITY CLASSIFICATION OF:	17. LIMITATION OF ABSTRACT Public Release	18. NUMBER OF PAGES 56	19. NAME OF RESPONSIBLE PERSON Fenster, Lynn lfenster@dtic.mil
---------------------------------	--	---------------------------	--

a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified	19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007
---------------------------	-----------------------------	------------------------------	--

REPORT DOCUMENTATION PAGE*Form Approved*
OMB No. 074-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE 3/1/2000	3. REPORT TYPE AND DATES COVERED Report 3/1/2000	
4. TITLE AND SUBTITLE Defense Message System Way Ahead: Conclusions and Recommendations from the Industry Advisory Panel		5. FUNDING NUMBERS	
6. AUTHOR(S) Unknown			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) DoD Industry Advisory Panel		8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) DoD Industry Advisory Panel		10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; Distribution unlimited		12b. DISTRIBUTION CODE A	
13. ABSTRACT (Maximum 200 Words) The DoD Industry Advisory Panel was formed to update the DoD Messaging Advisory Panel Report of 1997 with emerging technology trends and to provide recommendations on the way ahead in view of commercial directions in the next 2 to 5 years. This report presents our findings and recommendations, as well as background materials and summaries in the Appendices.			
14. SUBJECT TERMS IATAC Collection, defense message system		15. NUMBER OF PAGES 55	
		16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UNLIMITED

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18
298-102

Table of Contents

TABLE OF CONTENTS.....	I
1 EXECUTIVE SUMMARY.....	2
KEY CONCLUSIONS.....	2
<i>Messaging</i>	2
<i>Directory</i>	2
<i>Security</i>	2
KEY RECOMMENDATIONS.....	3
<i>General</i>	3
<i>Messaging</i>	3
<i>Directory</i>	3
<i>Security</i>	3
2 INTRODUCTION.....	2
PURPOSE.....	2
<i>Objectives</i>	2
SCOPE.....	2
<i>Market Segment</i>	2
<i>Time Frame</i>	2
<i>Technology</i>	2
<i>Perspective</i>	3
METHODOLOGY.....	3
INDUSTRY ADVISORY PANEL MEMBERS.....	3
3 CONCLUSIONS.....	4
GENERAL INDUSTRY VISION.....	4
▪ <i>PKI interoperability and consistency within specialized environments</i>	7
▪ <i>AES beginning to take hold in encryption mechanism solutions</i>	7
MESSAGING.....	7
<i>0 to 2 Years</i>	7
<i>2 to 5 Years</i>	7
<i>5+ Years</i>	8
DIRECTORY.....	8
<i>0 to 2 Years</i>	8
<i>2 to 5 Years</i>	9
<i>5+ Years</i>	9
SECURITY.....	9
<i>0 to 2 Years</i>	9
<i>2 to 5 Years</i>	10
<i>5+ Years</i>	10
4 INDUSTRY SCENARIOS.....	11
5 RECOMMENDATIONS.....	12
GENERAL.....	12
MESSAGING.....	12

DIRECTORY.....	13
SECURITY.....	14
<i>0-2 Years</i>	14
<i>2 to 5 Years</i>	14
<i>5+ Years</i>	14
INDUSTRY INFLUENCE	15
APPENDIX A: GLOSSARY OF TERMS	16
APPENDIX B: QUESTION AND ANSWER.....	17
MESSAGING.....	17
<i>Message Security</i>	25
<i>X.509 PKI Characteristics</i>	29
DIRECTORY.....	32
<i>Directory Services</i>	32
<i>Directory Security</i>	34
SECURITY.....	36
PUBLIC KEY INFRASTRUCTURE	36
<i>Certificate Generation</i>	36
<i>Interoperability</i>	36
<i>Certificate Revocation</i>	39
<i>Attribute Certificates</i>	40
<i>DVCS</i>	40
<i>Trusted Time</i>	41
<i>Cryptography</i>	41
APPENDIX C: GENERAL INDUSTRY TRENDS	43
INTRODUCTION.....	43
KEY MARKET DRIVERS.....	43
KEY MARKET TRENDS.....	43
ENTERPRISE PROBLEMS.....	44
CRITICAL SUCCESS FACTORS FOR THE ENTERPRISE.....	44
ENTERPRISE EXECUTIVE FOCUS.....	45
TOOLS FOR THOUGHT	46

1 Executive Summary

Key Conclusions

Messaging

- By 2002, most email systems will include SSL and S/MIME capability, with HTML/XML for rich content.
- There will be almost no use of X.400 within 3 years.
- By 2005 there will be more hand-held devices than desktop PCs. Planning must include provision for mobility and independence of medium.
- Communities of email users will have specialized security services deployed at the points where their email systems connect with the outside world in the 2 year timeframe.

Directory

- For the next two years, four simultaneous approaches to directory will continue:
 - ◆ general purpose directories
 - ◆ directory-enabled networks (DEN)
 - ◆ active directory (Microsoft)
 - ◆ X.500
- Over the next 2 to 5 years, X.500 will continue to evolve with the adoption of Internet and LDAP protocols into the standard. The result will be a much stronger technical alternative to standalone LDAP servers.
- It will take over five years for X.500 to blend into LDAP and eventually disappear.

Security

- Over the next two years, Public Key Infrastructure (PKI) will start to become a major element of email and messaging security.
- Smart cards are quickly approaching commercial. The basic security services they will provide over the next two years are identification and authentication.
- In the next two years, in cryptography, RC4 will dominate for the encryption of the Secure Socket Layer. 3DES is the likely near-term favorite for email. DES and RC2 will continue—as will PGP—for individual messaging and for some corporate enterprises. Products are now available for PGP at the corporate level. RSA will dominate the digital signature market, though DSA will continue to be available for some applications.
- In 2 to 5 years, users will require multiple identities and roles in all communities of interest, not just DoD, which will lead to broader support by commercial product providers for multiple certificates to reflect these roles and identities.
- Also in 2 to 5 years, smart cards will dominate in the cryptographic token market, used to carry PKI certificates for all types of security services including access control, confidentiality, integrity, and non-repudiation.
- It may take over five years before PKI will be available for interdomain communications of all types and will be very mature and interoperable.

Key Recommendations

General

- Join forces with enterprises solving similar messaging problems to create new market sectors with requirements in common with DoD.
- Conduct further study of the impact on DMS decisions of the ISP/ASP model and messaging middleware.

Messaging

- Begin to transition X.400 technology to SMTP technology immediately.
- Develop a coexistence strategy immediately while planning migration to S/MIME in the next 2 to 5 years.
- Investigate SSL and secure staging servers, or products that create secure “packages” that can be delivered to new users as a possible short-term way of providing secure messaging.

Directory

- Allow the incorporation of LDAP-compliant directories immediately at the edges of the DMS directory system, including Active Directory, NDS and LDAP based directories such as iPlanet (Sun/Netscape Alliance).
- Continue to utilize an X.500 backbone for the next 2 to 5 years.
- Begin transitioning the X.500 backbone to a new technology in 3 to 5 years.

Security

- Over the next 2 years, adopt as much commercial security as feasible; potentially redesigning portions of the DMS or DII architectures to enable separation of sensitive but unclass information from classified information.
- In the next two to 5 years, transition to use of AES algorithms and migrate to standards-based smart cards.
- In 5 years time, initiate business agreement cross-certification with Federal and industry entities and begin using PKI mechanisms for business grade legal documents.

2 Introduction

Purpose

The DoD Industry Advisory Panel was formed to update the DoD Messaging Advisory Panel Report of 1997 with emerging technology trends and to provide recommendations on the way ahead in view of commercial directions in the next 2 to 5 years.

This report presents our findings and recommendations, as well as background materials and summaries in the Appendices.

Objectives

The Industry Advisory Panel objectives are to:

- Update DoD Messaging Advisory Panel Report with new trends in messaging, directories and security technology.
- Examine parallels in large-scale commercial enterprises (including commercial service provider models).
- Evaluate commercial market support for key DoD requirements.
- Highlight emerging trends in Internet protocols and make recommendations on the viability of DMS protocols.
- Recommend how to enhance/influence commercial development activities.
- Address key security technologies and provide recommendations.
- Consider industry directory topology and technologies.

Scope

The scope of the research and recommendations are as follows:

Market Segment

- Focus on enterprise trends and requirements.
- Discuss *industry* requirements and trends as opposed to the government sector.
- Examine trends and requirements from a global perspective.

Time Frame

- Provide perspective in two time frames, 1–2 years and 2–5+ years.

Technology

- Focus on messaging, directory and security areas.
- Messaging includes person-to-person, person-to-application and application-to-application messaging.
- Include other (non-email) applications and processes as they relate to messaging.
- Examine areas in industry where there are requirements for high security and identify developments to address these requirements.
- Limit research and recommendations pertaining to implementation issues.

Perspective

- Conclusions are based on the knowledge base of the participants and the research conducted within the limited time frame of the contract.
- The level of detail provided will be comparable to the previous report of 1996; supporting reference will be included in the Appendix.

Methodology

The Panel employed the following methodology:

- The Panel received a briefing from The Defense Message System Program Office, then met with the DMS Technical Working Group to clarify scope, focus and objectives.
- The first draft of results were developed then reviewed and discussed by the entire panel.
- High level scenarios and trends were developed and discussed with the entire panel.
- Detailed events and trends—along with their impact—were identified for each technology sector: messaging, directory and security.
- The first draft of the report was developed and will be reviewed by the panel and the DMS Technical Working Group.
- Edits and comments will be incorporated by the panel and a presentation and final report completed.

Industry Advisory Panel Members

Alexis Bor, President and CEO, Directory Works, Inc.

Nina Burns, President and CEO, Creative Networks, Inc.

David Ferris, Sr. Analyst, Ferris Research

Natalie Givans, Principal, Booz-Allen & Hamilton, Inc.

Joyce Graff, VP and Research Director, The Gartner Group

3 Conclusions

General Industry Vision

According to the Gartner Group several important trends will affect the evolution of messaging, directory and security over the next several years. These predictions are put forth by the Gartner Group. Although the Industry Panel has not necessarily reached consensus on the specifics of these issues, they are included because the general trends are significant.

- By 2001, the North American market for outsourcing messaging services will grow to \$2.6 billion (0.7 probability,).
- By year-end 2002, at least 50 percent of enterprises will outsource at least 25 percent of their email budget (0.8 probability).
- Through 2005, unification of messaging, voice and fax will be a major factor in 30 percent of messaging outsourcing decisions (0.8 probability).
- Mass access device (MAD) shipments will exceed PC shipments by year-end 2005 (0.6 probability).
- Through 2005, architecture of unified messaging products will evolve from integration of existing hardware and software modules to single-purpose servers (0.8 probability).

As the number of implementations rise the number of highly-trained and highly-skilled people will be insufficient to staff all locations. Thus the systems have to be manageable from remote locations, or by less skilled staff. In industry this is driving centralization, simpler products, or outsourcing. There may well be a desire on the part of small components to outsource their messaging. DMS may wish to encourage one or more vendors to create a secured outsourcing option for these units, or may wish to do that themselves.

These predictions will be driven by a number of market factors over the next 5 years as the digital economy and the transformation to e-business increasingly influence the direction of electronic messaging. The role of messaging in e-business stretches the boundaries of the traditional role of messaging in a variety of ways. Email and messaging will become a critical factor in many areas, particularly those outlined below:

- Internal (Intracompany) Communication: Email will provide a reliable distribution highway and infrastructure for process automation
- Knowledge Repository: Today 45 percent of useful business information is stored in the messaging system (Creative Networks, 1999), causing information overload. There is a driving the need for better ways to store, retrieve, and leverage this information.
- External Information: Email provides a communication conduit to partners/suppliers/customers and an underpinning launchpad for e-commerce applications, especially in areas such as customer service, customer interaction, customer care and customer relationship management.

- **Extended Enterprise:** Email will rapidly become a primary communication medium for general and critical business correspondence as well as a critical infrastructure for automated global business processes.
- **Electronic Commerce:** Email is already a primary notification and alert and customer interaction infrastructure.
- **SMTP/S-MIME** has some important shortcomings, many of which are addressed by the messaging middleware software discussed elsewhere in this document. For example, there is no guarantee that email will be delivered within a certain time, and or that delivery receipt will be received even if the message has been successfully delivered. Thus organizations will not rely on email as the sole means of communication with people. They will also use other channels.

The result of these influences is a landscape quite different from that of today in many ways. The following chart provides a snapshot of the key aspects of email, directories and security over the next 5 years (we have distinguished between email and messaging middleware in the chart).

Email	
0–2 years	<ul style="list-style-type: none"> ▪ Instant messaging is pervasive ▪ Focus on remote user access, multiple devices ▪ High demand for wireless access (1–2 years)
2–5 years	<ul style="list-style-type: none"> ▪ Wireless access widespread ▪ Unified messaging pervasive ▪ Security/privacy dependent on service provider
Long-term	<ul style="list-style-type: none"> ▪ Highly reliable systems generally available ▪ Authentication will be critical ▪ Wireless, portable, choice of medium, everywhere, every time ▪ Appropriate security everywhere
Messaging Middleware	
0–2 years	<ul style="list-style-type: none"> ▪ Commercial ISPs will provide messaging middleware services ▪ ASPs will provide messaging middleware services ▪ Part of integrated application architecture ▪ OCSP services generally available
2–5 years	<ul style="list-style-type: none"> ▪ Highly distributed applications are pervasive ▪ Interoperability provided through deployment of messaging middleware architectures
Long-term	<ul style="list-style-type: none"> ▪ Messaging middleware becomes a key component of intelligent networking, which will be available on a global scale
Directory	
0–2 years	4 simultaneous directory approaches: <ul style="list-style-type: none"> ▪ general purpose ▪ directory-enabled networks

	<ul style="list-style-type: none"> ▪ active directory ▪ X.500 ▪ LDAP is the standard interface ▪ X.500 still provides server-to-server backbone services
2–5 years	<p>The four approaches begin to converge</p> <ul style="list-style-type: none"> ▪ X.500 rapidly displaced by other alternatives, particularly LDAP and Active Directory ▪ First instances of directory-enabled networks (DEN) emerge ▪ Widespread availability of web based directories with rapid access and high performance
Long-term	<p>All 4 converge on single directory approach:</p> <ul style="list-style-type: none"> ▪ undefined ▪ DEN

Security	
0–2 years	<ul style="list-style-type: none"> ▪ PKI pilots widespread, no consistency or interoperability ▪ Multiple, disparate cryptographic algorithms continue ▪ Rudimentary access controls ▪ User application security relies heavily on network protection mechanisms (e.g., FW, IDS, VPN)
2–5 years	<ul style="list-style-type: none"> ▪ PKI interoperability and consistency within specialized environments ▪ AES beginning to take hold in encryption mechanism solutions ▪ Smart cards pervasive for PKI certificates and other user data
Long-term	<ul style="list-style-type: none"> ▪ PKI interoperability interdomain with cross-certification ▪ Cryptographic algorithm consistency for multiple integrated applications ▪ Users identified, authenticated, and granted access across multiple domains, in multiple roles- reflected in messaging and email protocols

Messaging

0 to 2 Years

- By 2002, most email systems will include SSL and S/MIME capability, with HTML/XML for rich content.
- Web user interfaces will be the norm for corporate email users.
- Over the next 2 years users will be able to choose the medium (e.g., fax, email, or voice) and device (e.g., computer, phone, or fax machine) that best suits their needs for sending or receiving messages.
- The message store will be integrated with other corporate information stores, such as the file system and knowledge management systems.
- Messaging middleware will emerge as a separate and well-understood application integration and application-to-application communication.

2 to 5 Years

- There will be almost no use of X.400 within 3 years.
- Wireless handheld devices will be easily and commonly integrated with corporate messaging systems.

- Instant messaging will be very popular in large organizations. It will not, displace email but will become a useful adjunct with integration with other media types as part of unified messaging
- Email and other information sources, stores and interfaces will converge (such as Enterprise Information Portals and Knowledge Management Systems).
- A solid infrastructure of messaging middleware will provide interoperability and highly distributed applications in integrated application architectures. This will be separate from the corporate email system.
- Communities of email users will have specialized security services deployed at the points where their email systems connect with the outside world. These services will include virus control, spam blocking, and protection against malicious attacks.

5+ Years

- Communities of email users will have specialized security services deployed at the points where their email systems connect with the outside world. These services will enforce corporate policy, and will add content filtering, control of large files, and internal and external chargeback.
- Unified messaging appliances (including media and device) will become commonly used equipment maintained on customer premises.
- Messaging outsourcing will be common in large organizations.
- Most people in developed countries that are age 6 or older will have an email address.
- Most large organizations will have deployed automated email response management systems.
- The current dichotomy between a hierarchical file system and a hierarchical message store will disappear. It will be replaced by a more general-purpose object store, and this will more readily allow information to be accessed by other people in the organization.
- URL pointers, rather than file attachments, will be normally used to provide file access. This will reduce errors associated with multiple file copies, and will reduce the average size of messages.
- Services providing priority delivery, assurance of delivery and non-repudiation will be commonplace options for business and consumers alike. Intelligent networking and messaging middleware will provide some of these services.

Directory

0 to 2 Years

- Four simultaneous approaches to directory will continue:
 - ◆ general purpose directories
 - ◆ directory-enabled networks (DEN)
 - ◆ active directory (Microsoft)
 - ◆ X.500
- The dominant technology will be LDAP V3, followed by an evolution of LDAP into a newer generation of functionality and capability.

- LDAP has already established itself as the de facto interface used by applications into directory systems. LDAP will continue to be the de facto interface used by applications, but a number of vendors will encourage users to use their proprietary interface. A number of exciting features and functions will be added to these proprietary interfaces in an attempt to lock users into a single proprietary solution.
- X.500 will still provide some server-to-server services not available from other technologies and is therefore a valuable component on the backbone.
- Email will lose its status as the primary driver and consumer of directory technology.

2 to 5 Years

- X.500 will continue to evolve with the adoption of Internet and LDAP protocols into the standard. The result will be a much stronger technical alternative to standalone LDAP servers.
- LDAP standards will incorporate X.500 server to server capabilities.
- There will continue to be significant chaos in the directory market.
- No single directory approach will dominate the landscape, but major players will continue to evolve their products and differentiate themselves with additional non-standard features.

5+ Years

- Market pressures take over and X.500 will blend into LDAP. X.500 will eventually disappear from the landscape .

Security

0 to 2 Years

- Public Key Infrastructure (PKI) will start to become a major element of email and messaging security as it matures to provide user identification, authentication, access control, and enables key distribution for confidentiality, integrity and availability.
- PKI pilots will be widespread. However, each pilot will be for a local environment (intra-domain), using a homogeneous PKI product line during this period.
- Digital signatures will be commonly used to bind timestamps to email, messages, and other application information.
- PKI will not be interoperable across domains for a variety of reasons, including Certificate Authorities (CAs) not being able to cross-certify, certificate revocation being immature, and certificate generation methods being non-interoperable.
- Smart cards are quickly approaching commercial viability as multi-function devices for access control, card swiping, and credit/debit purchases, in the insurance, health care, and banking domains, for example. The basic security services they initially provide will be identification and authentication.
- In cryptography, RC4 will dominate for the encryption of the Secure Socket Layer. 3DES is the likely near-term favorite for email. DES and RC2 will continue—as will PGP—for individual messaging and for some corporate enterprises. Products are now available for PGP at the corporate level. RSA will dominate the digital signature market, though DSA will continue to be available for some applications.

- Many pilots adopt simplified service provider approach to secure messaging as crude stand-in for general desktop-to-desktop secure messaging.

2 to 5 Years

- Users will require multiple identities and roles in all communities of interest, not just DoD, which will lead to broader support by commercial product providers for multiple certificates to reflect these roles and identities. Current systems support use of different certificates such as one for authentication and one for confidentiality. This will not be sufficient as users participate in multiple domains/communities of interest, based on either classification levels or mission areas (e.g., logistics, command and control, personnel, financial).
- Commercial products will support dynamic secure communities where the membership in a community will change to reflect the current mission need. Products will enable a user to be mobile and to join or leave communities dynamically based on their job function and role.
- Smart cards will dominate in the cryptographic token market in this time frame, used to carry PKI certificates for all types of security services including access control, confidentiality, integrity, and non-repudiation. Because they will become critical to inter-domain email and messaging, the interface between smart cards and applications will migrate to standard APIs driven either by the smart card vendors, by the operating systems, or both.
- PKI will mature such that different domains will be able to interact where necessary through selective cross certification and availability of standards that ensure PKI and certificate compatibility and interoperability across domains.
- The Advanced Encryption Standard will have been selected by this time and products will be implementing the winner or winners. At least 2 of the 5 current finalists are expected to dominate the market—one U.S.-based algorithm and one foreign-based algorithm. It is reasonable to expect that many DES and 3DES applications will migrate to AES.

5+ Years

- PKI will be available for interdomain communications of all types and will be very mature and interoperable. Vendors will work together to achieve this goal, much as the Automated Teller Machine (ATM) market evolved once it was clear that vendors increased market share by being widely interoperable. Cross certification will be ubiquitous.
- Assured service for email and messaging, as well as other applications, will be provided through network protocols and network management and switching devices. Assured service means that availability, integrity, and possibly confidentiality requirements will be specified by an application or an enterprise on a granular basis and will be provided through the network configuration and processing elements.
- PKI-based non-repudiation, used for legal admissibility of signed transmittals and receipts will be available.

4 Industry Scenarios

Following are industry scenarios that present challenges similar to those faced by Defense Message System.

- **Enterprises, conglomerates, or industry groups made up of multiple autonomous constituencies.** While there are common goals, there is local control of the P&L and the budget priorities.
- **Banks** making funds transfers B2B, or handling transaction requests and funds allocations involving consumer input (teller machines, at-home banking). New customers must be “authenticated”—Is this person real? Is he who he says he is?—and must receive account details in a secure package, protected from “sniffing” on the Internet.
- **Enterprises in the transportation industry, or mining and drilling, rescue or police operations,** needing to deploy teams into thinly-settled or foreign territory with no existing (or reliable) infrastructure of telephony and data connectivity. Secure transmission over satellite links or other wireless options.
- **B2B and B2C sales** over the Internet, conducting business over an inherently insecure infrastructure. Need for authentication and data security. What is at risk is usually money—not lives and national security—so “good enough” is usually a lower threshold. But the issues are similar.
- **Brokerage firms,** particularly those competing for the online brokerage business, may exhibit strong requirements for time-sensitive messaging for applications such as notifying clients of changes in activity on a stock.
- **Multi-national enterprises** doing business in many countries, some of which are hostile, or whose governments encourage industrial espionage and theft. There is need for worldwide data protection at a high enough level that well-funded criminals and foreign governments cannot break the codes.
- **Businesses exchanging** orders, confirmations, credits, debits, funds transfers, and other documents (traditional electronic data interchange) requiring absolute assurance of delivery, in the correct sequence, once and only once, rely on Messaging Middleware to perform these services which cannot be assumed in Email.

5 Recommendations

General

- A further study should be undertaken, to review the DMS-desired capabilities in the following areas:
 - Message priority flags, minimum of 2 levels (e.g., X.400 priority which determines the priority/order of processing of the message by the infrastructure)
 - Message Importance Indicator (e.g., what is the importance of the message from the end user perspective)
 - Delivery and Non Delivery Notices from the recipients mail host
 - Proof of Origin (authenticate who sent the message)
 - Proof of Receipt
 - Integrity of Message Data
 - Confidentiality of Message Data
 - Message level access controls (will forward GENSER MILCOM '99 Paper as background on this topic)
 - Auditability
 - Alternate Delivery (Directory and Messaging System)
 - Capability to differentiate between Organizational Messages and Individual Messages

This study should examine these requirements, with an eye to aligning them with similar industry requirements, so as to form a coalition of interests that will be an attractive segment for vendors.

- As experience has shown, levying special requirements on top of COTS products results in custom products with the same problems as products custom-built from scratch. Another approach is to join forces with enterprises solving similar problems, to create new market sectors with requirements in common with DoD, sufficient to motivate vendors to design and sustain COTS products for the entire market sector.
- Further study should be made to understand the impact of the ISP/ASP market and channels.
- Further study should be made to understand the emergence and impact of messaging middleware.

Messaging

- New investments in X.400 technologies of all types has effectively ceased by the industry. However companies with existing X.400 implementations continue to rely on them to do

things that SMTP products cannot yet do. DOD needs to begin to replace this technology immediately. Gating factors will be the availability of vendor support for the existing products, and the cost and availability of alternative technologies.

- Migration to S/MIME will not take place overnight. Therefore, a coexistence strategy is required. This normally entails using an X.400-to-S/MIME gateway. Secure messages cannot pass through a gateway since the reformatting of the message itself breaks the checksum on the message. However, secure content can be passed successfully through a gateway today. DOD should immediately start planning its coexistence strategy to determine suitable options.
- For the next five years, SMTP messaging (with or without S/MIME) will lack certain reliability features, such as delivery within a specified time, and the guarantee that if a message has been delivered, that a notification can be returned. DOD will need to plan how to identify the subset of messages that have these requirements, and the mechanism to be used to satisfy them.
- Enterprises with immediate requirements for secure interpersonal messaging (e.g. banks sending account details to new customers) are solving this problem today with SSL and secure staging servers, or with products that create secure "packages" that can be delivered to new users. These should be investigated as a possible short-term way of providing secure messaging, especially with people with a low percentage of DMS usage who are resisting implementation of the full DMS infrastructure.
- Ever-growing needs for mobility and unified messaging will drive additional requirements. The wireless community is already working with requirements for unique identifiers, position location, and secure transmissions, for 911, police, funds transfer (e.g. PayPal.com) and credit card purchasing. Adding DoD requirements into this space will not be difficult (e.g. reading a secure email message by voice over a wireless phone) because of the logical alignment of these requirements with commercial requirements.

Directory

- Pure X.500 directories are tapering off rapidly. Longer term, there are two major industry initiatives, Microsoft Active Directory and LDAP distributed directories. While X.500 still provides some server-to-server services not available from other technologies and is therefore a valuable component on the backbone, many companies, departments and organizations with separate decision-making powers will resist purchasing X.500 components due to cost and complexity. The directory infrastructure for DoD must therefore allow for the immediate incorporation of other LDAP-compliant directories at the edges of the DMS directory system, including Active Directory, NDS and LDAP based directories such as iPlanet (Sun/Netscape Alliance).
- These initial implementations may apply to new and or peripheral deployments and integrate into the X.500 backbone. A second step, beginning deployment in the 3 to 5 year timeframe should focus on transitioning the X.500 backbone to a new technology.
- DoD should track and guide the development of industry standard server-to-server protocols as a next-generation solution for the X.500 services set. Standards will not be adequately defined until approximately 2002, with interoperable commercial products available by 2003.
- Microsoft's Active Directory is an unknown quantity and may well become very important: the DOD should, effective immediately, maintain a good understanding of the state of this technology, in order to determine if and when it should be incorporated into DMS.

Security

0-2 Years

- Identify industries with secure messaging and email requirements similar to DoD requirements and follow their lead with implementing flexible, scalable, transition solutions .
- Industries/applications with similar confidentiality requirements include banking, energy, and transportation (e.g., air traffic control, air transportation safety)
- Industries/applications with similar integrity requirements include financial services and e-business, health care, insurance, and legal.
- Industries/applications with similar availability requirements, including time criticality, include e-business, stock traders, air traffic control.
- Participate in industry and Government security venues such as IETF-PKIX and the Federal PKI Technical Working Group, respectively, to influence standards and product features.
- Participate in industry interoperability forums such as the PKI Forum to encourage interoperability between commercial vendors.
- Adopt as much commercial security as feasible; potentially redesigning portions of the DMS or DII architectures to enable separation of sensitive but unclassified information from classified information so that the bulk of DoD communications that is SBU can be handled with commercial solutions and associated assurances similar to those required by industry.
- Initiate research on the practical use of certificate policy mechanisms to convey various levels of assurance.
- Initiate research on the use of attribute certificates as a method for conveying authorizations.

2 to 5 Years

- Transition to use of AES algorithms
- Migrate to standards-based smart cards
- Encourage research on business-grade cross-certification applications
- Encourage development of legal framework to accept digital signatures on business grade agreements

5+ Years

- Initiate business agreement cross-certification with Federal and industry entities

- Begin using PKI mechanisms for business grade legal documents
- Implement sophisticated rule-based access control utilizing attribute certificates based on commercial standards
- Transition to fully COTS-based infrastructure; utilize COTS applications to fullest extent.

Industry Influence

There are several ways the Advisory Panel would suggest that the DMS Technical Working Group consider to influence the direction of industry. These include:

- Participation in standards bodies and working with the providers of the most broadly deployed freeware products (Sendmail, Qpopper, and Apache) could result in raising the quality of the Internet as a whole and the baseline of available services in the protocol. For example, the availability of receipts was a primary requirement for making the Internet “good enough” for business. This functionality was 90 percent deployed throughout the Internet in 9 months thanks to its inclusion in the freeware product Sendmail. In the standards bodies, it will be important to form coalitions with enterprises that share common concerns, and to listen carefully to their requirements, not simply to work a particular agenda. Go with problems, not with solutions.
- Publish DMS solutions to the industry for general usage. The idea here is to provide technical documentation and models freely to the industry, which enterprises with similar requirements can adapt to their needs. The effect of this is educational as well as a “bottom up” approach to influencing industry direction.
- Government can play an important role in setting up a PKI and a global network of CAs. This could be tied in with the international treaties and police agreements that surround things like passport conventions and Interpol agreements. Some countries will be more cooperative than others will, but a global “hierarchy of trust” will be able to highlight CAs that are less than credible. This would go a long way to facilitating international commerce as well as obtaining the product capabilities of interest to Defense.
- Restriction on export of security protocols only promotes invention of additional protocols by competing parties worldwide. Because business (especially international banking) also needs high levels of security, cooperation with industry in deploying cryptography for global use could result in the availability of COTS products at a reasonable price that would meet the security requirements of Defense.

Appendix A: Glossary of Terms

To be completed in Draft 2.

Appendix B: Question and Answer

This section is unedited. It will be completed in Draft 2.

Messaging

1. What technologies and architectures will business and industry employ to build high performance, robust, reliable, and secure messaging systems over the next 2 years?

Trends

- SMTP/MIME has captured the market place as the WAN messaging protocol of choice.
- The major enterprise vendors, Lotus, Microsoft, and Novell, are converting their proprietary formats to S/MIME, with rich text represented by HTML.
- PGP has a presence. Academics often use it. Also individuals often use it for ad hoc secure messaging. However, commercial pilots rarely opt for PGP, they almost always go for S/MIME or alternative solutions (such as Israeli crypto and staging)
- The PGP (informal web of trust) and X.509 (global hierarchy of CAs) trust models are converging. For example, industry groups such as Indentus, and VeriSign are defining certificate issuance and management practices across clusters of organizations.
- S/MIME is currently hampered by the price of using RSA's patented encryption algorithm. The patent expires in September 2000, which will neutralize this argument.
- Many enterprises will initiate key infrastructures within the enterprise as part of the deployment of Lotus Notes R5 and Microsoft Exchange 2000.
- Commercial enterprises want to be able to conduct secure electronic commerce transactions with individuals and other businesses over the Information Highway. As far as secure messaging goes, that means they hope to have desktop-to-desktop services available. Many enterprises will do secure messaging pilots during 2000 and 2001.
- Most people will find that there are more implementation issues than they care to tackle. They will often choose work-around compromise solutions such as staging services or boundary-to-boundary security.
- Public key infrastructures within industry groups will develop slowly, beginning with site-to-site security by 2001, and growing to person-to-person security by 2005.
- Boundary messaging services, close to corporate firewalls, are growing much richer. Services include anti-virus, anti-spam, keyword filtering, auto-signing, auto-encryption, user chargeback.
- Some commercial encryption approaches will involve boundary (site-to-site) encryption.
- Financial services organizations and government will be early adopters of secure messaging. Health care businesses will be too, but they often will have less technical sophistication. Drivers include the risk of heavy fines for failure to take sufficient steps to protect patient confidentiality and client financial details.
- Companies are beginning to outsource their email systems. By 2005, large organizations will commonly outsource much or all of their email systems. Smaller organizations, especially the more distributed ones, are more ready to outsource than larger ones' email.
- Call centers and busy offices are implementing specialized types of email systems (ERMS), from vendors such as Kana, Brightware, eGain. These are growing rapidly and are

an important class of product. They perform such functions as automatically sorting messages depending on their content, routing to operators, building a knowledge base and preparing draft replies, and compiling management reports on the volume and type of messages handled.

- 128-bit security will be common internationally as of 2002.

Issues

- S/MIME slow to roll out because of implementation complexities and lack of an interoperable PKI.
- Through the combination of how TCP/IP works, common Domain Name System naming conventions, and the log files kept by ISPs and Web site operators, it is possible for someone to trace messaging patterns. Although they may not be able to read message content, inferences can be made by means of traffic analysis and related disciplines.

Relevant Standards and Protocols

- RFC 821: Simple Mail Transfer Protocol (SMTP)
- RFC 822: Standard for the format of ARPA Internet text messages -- being updated
- RFC 974: Mail routing and the domain system (MX records)
- RFC 1869: SMTP Service Extensions
- RFC 1870: SMTP Service Extension for Message Size Declaration
- RFC 1939: Post Office Protocol - Version 3 (POP3)
- RFC 2045: MIME Part 1: Format of Internet Message Bodies
- RFC 2046: MIME Part 2: Media Types
- RFC 2047: MIME Part 3: Message Header Extensions for Non-ASCII Text
- RFC 2048: MIME Part 4: Registration Procedures
- RFC 2049: MIME Part 5: Conformance Criteria and Examples

Direct Answer

- Secure SMTP/MIME (S/MIME) is expected to be the primary way that secure person-to-person messaging systems will be put in place. However, between 2000 and 2002, secure email deployments including external connectivity will be rare. There will be significant internal key infrastructures (especially on Lotus Notes R5, Microsoft Exchange 2000, Novell Groupwise, and Netscape/iPlanet) and many inter-enterprise pilots especially within industry and e-commerce groups, but little consumer deployment.
- Meanwhile, SSL will be used to protect data from point-to-point both in B2B and B2C transactions. SSL can be used to protect messages deposited on a secure "staging" server; regular email used to send a notification to the recipient, and SSL used to protect the data as the recipient picks it up from the staging server. The data may be stored in an encrypted form on the staging server, and decrypted on pickup. Products in this space include Tumbleweed, Ziplip, and Click2Send.
- Because of difficulties in global deployment of keys lengths greater than 40 bits, vendors in other parts of the world have created alternative solutions for problems of point-to-point

security. Examples include Aliroo (Israel) and Baltimore and Viasec (Ireland). With the liberalization of export restrictions S/MIME will be more broadly deployed, but these offshore solutions will continue to have their niche in the market.

- LDAP will be implemented to support access to certificate repositories and other directory functionality. LDAP is already very widely deployed and is usable now to store, access, and manage certificates.
2. What is the impact of market segmentation into enterprise messaging (functionality driven) and ISP email (scalability driven) on DMS? What mix of services should we provide?
- First, a couple of definitions. “enterprise messaging (functionality driven)” = products such as Lotus Notes, Microsoft Exchange, Novell Groupwise, Netscape/iPlanet. “ISP email (scalability driven)” = products like Netscape/Sun/iPlanet, Software.com, MessagingDirect, Innosoft, Oracle, Sendmail Inc.
 - In any large enterprise there are users who require a rich set of groupware features—and other users who require no more than simple email. In DMS, because of the requirements for security and authentication, the bar begins at a higher level than the average ISP would use to provide basic email. DMS product choices will necessarily meet the following requirements:
 - Interact seamlessly with Internet users via SMTP/MIME protocols “in the clear”
 - Provide ease of use when corresponding with recipients requiring optional authentication.
 - Provide easy-to-use mechanisms to view and validate the credentials presented by correspondents.
 - Provide access to the optionally required level of security
 - The general trend, within enterprise messaging as well as ISP products, is to add functionality. By 2005, and perhaps sooner, ISP mail can be expected to incorporate S/MIME services using a world-wide PKI. These should be useable by DOD users not needing high-end secure messaging capabilities. Shorter term, specialized service providers will offer alternative methods for secure messaging such as SSL and secure staging servers. These may provide a short-term, stop-gap solution for some DOD users not needing high-end command and control messaging.

Trends

- Basic ISP mail today usually has quite a lot less function than enterprise email systems, and the Web UIs are cumbersome. Premium outsourced services generally have higher levels of email functionality than internal systems and often lure traveling users to forward their corporate email to an external service.
- Web-based User interfaces will become much better over the next couple of years, adding such functions as drag-and-drop and optional local file cabinet.

Issues

- “Webmail” is cheap. Some ISPs will offer secure messaging (e.g., Tumbleweed), and this may be attractive as a tactical means to offer ad hoc secure messaging, to companies put off by the complexity of their pilots.
- The new Instant Messaging and Presence Protocol (IMPP) is not yet developed and available. However products currently exist to provide Instant Messaging for enterprise

deployment (Lotus Sametime, iPlanet AIM) that are committed to interwork with and migrate to IMPP.

Relevant Standards and Protocols

- Same as those in 1 above.
3. What will the impact of Web-based front ends for electronic mail (i.e., so called "Web Mail") be on the electronic mail market?

Trends

- They are very widely used by consumers. So-called Web mail is expected to have 131 million users and generate 561M messages per day by 2002, according to one source.
- The entire free email paradigm is based on user willingness to tolerate advertisements in return for free usage.
- While free accounts are funded through advertising (and the user "pays" with attention cycles), enterprise outsourcing services and products such as Infonet's MailMail provide very nice Web interfaces WITHOUT advertising (for a price per month). Web interfaces provide the option of including other network ASP services (e.g., enterprise messages, news feeds, dynamically updated content, refreshed whenever the URL is hit, or more often using dynamic banners.) The major enterprise vendors are all moving toward a Web paradigm (Lotus Notes R5, Outlook Today, Novell Groupwise Web Access, Netscape Java Development Kit, etc.).
- Corporations would like to use Web UIs if they can, to access their Domino or Exchange mailboxes, because the administration efforts are much less.
- High bandwidth is important for a satisfactory Webmail experience.
- High volume email users will prefer not to use Webmail as their full-time client for the next 2 or 3 years.
- A growing number of wireless devices, portable data telephones, and other PDAs will depend upon Web interfaces to access email and other applications on the Internet. Web interfaces will evolve to be able to dynamically self-modify based on the device capabilities (number of lines, width of screen, font and image capabilities).

Issues

- A Web mail front-end could serve tactical requirements if appropriate security is implemented. One example would be kiosks in patient care areas in hospitals, where doctors can check their messages. They have to have a "panic button" to hit when they are called away on an emergency, shutting down the email account and purging all buffers to protect patient confidentiality.
- The same issues with regard to PKI for S/MIME (see responses to 8 and 9 below) apply to Web mail.
- Web UIs today lack a number of features that users expect in platform-specific clients, (e.g., drag and drop). However, its functionality is good enough for many users (e.g., flight crew, truck drivers in the garage), especially when weighed with the advantages in mobility and remote access

Relevant Standards and Protocols

- HTTP and HTML, WML, WAP, XML

Direct Answer

- Web front-ends to email will become increasingly important in enterprises, often connected to Domino or Exchange servers. While they will not be used as the primary interface for full-time professional information workers during the next two years, they will become the interface of choice for certain conditions and classes of users:
 - To serve the class of users traditionally supported with green screens. Web front-ends provide an inexpensive, always-connected interface, which is easily updated without installing any software on the desktop device. In this way, thousands of users can be updated to a new version within an hour, simply by installing the next release on the server. The next time the user hits the URL, the latest version is in place and ready for use.
 - For kiosk applications, in areas where multiple people share a single terminal (assembly floors, garages, patient care areas in hospitals, etc.)
 - To provide remote access for people not at their desks, in another part of the building, or on the road (kiosks in public areas, WebTV in hotel rooms, etc.)
 - To provide remote access for the full range of wireless devices.
4. Where is the explosion in character set capability and other advanced formatting features (e.g., XML, embedded graphics and objects) headed? Will interoperability be possible? What standards will dominate?

Trends

- The World Wide Web Consortium with 390 members is leading the way toward standards-based, platform-independent rules for handling structured data.
- XML will underpin a number of Web markup languages including HTML and will include definitions for handling embedded graphics and objects.

Issues

- XML 1.0 contains the latest rules and conventions that put structured data such as spreadsheets, address books, configuration parameters, financial transactions, technical drawings, etc. into text format to enable users to look at the data without the program that produced it. Unlike HTML, tags have different meanings in different contexts.
- XML 1.0 is a family of features and implementations to solve a range of issues. XML 1.0 includes Xlink, describing a standard way to add hyperlinks to an XML file; XPointer & Xfragments, syntaxes for pointing to parts of an XML document; CSS, the style sheet language; XSL the advanced language for expressing style sheets; DOM, a standard set of function calls for manipulating files from a programming language; XML Namespaces, specifying how to associate a URL with every tag and attribute in an XML document; XML Schemas (1 and 2), helping developers to precisely define their own XML-based formats.
- XML 1.0 should redefine and expand interoperability with regard to character sets, embedded objects, etc. in a way not previously accomplished.

Relevant Standards and Protocols

- *RFC 1766: Tags for the Identification of Languages*, 1995.
- RFC 2376: XML Media Types.
- *ISO 639:1988: Code for the representation of names of languages*. [Geneva]: International Organization for Standardization, 1988.
- *ISO 3166-1:1997: Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes* [Geneva]: International Organization for Standardization, 1997.
- *ISO/IEC 10646-1993: Information technology -- Universal Multiple-Octet Coded Character Set (UCS) -- Part 1: Architecture and Basic Multilingual Plane*. [Geneva]: International Organization for Standardization, 1993 (plus amendments AM 1 through AM 7).
- *ISO 8879:1986: Information processing -- Text and Office Systems -- Standard Generalized Markup Language (SGML)*. First edition -- 1986-10-15. [Geneva]: International Organization for Standardization, 1986.
- *ISO/IEC 10744-1992: Information technology -- Hypermedia/Time-based Structuring Language (HyTime)*. [Geneva]: International Organization for Standardization, 1992. *Extended Facilities Annexe*. [Geneva]: International Organization for Standardization, 1996.

Direct Answer

- From 2002, XML will be the standard to allow industries to define platform-independent protocols for the exchange of data, especially the data of electronic commerce, and allow information to be displayed as the user wishes. XML will be used for client/server interactions with back-end data structures, and will be used for malleable data formatting for devices other than desktop PC's.
5. How are "groupware" features (e.g., scheduling, newsgroups, document sharing) likely to interact with or integrate with traditional electronic mail?

Trends

- The main new features being added and integrated are: group scheduling, rich directories, forms routing, instant messaging, presence information, news groups/shared folders/bulletin boards, document management, fax servers
- Directories are central to the provision of these new functions.
- There's much talk about unified messaging (integrated access to email, fax messages, voicemails, pager for sender and recipient) but little corporate premises purchases at least through 2002. Unified messaging is being sold primarily one portable telephone at a time.

Service offerings are evolving rapidly; the technology will obsolesce rapidly, causing most enterprises to defer premise purchases until at least 2002.

- Message stores are evolving into rich repositories of information. Storage by person inhibits retrieval and reuse by the enterprise as a whole. Increasingly sophisticated search, document management, knowledge management, and archiving tools are needed.
- Because of the ubiquity of the SMTP/MIME infrastructure, groupware tools that aspire to operate across diverse systems often rely upon email as a conveyance for structured data. Example: The ical standard for calendar interworking relies upon email as a conveyance for structured text messages. Other common infrastructure components for groupware are HTML and SSL.
- Enterprise email vendors are increasingly adding groupware features (including business card presentation, calendaring, newsgroups, etc.) to their email packages. If history is a teacher, there is a limit to the richness that users will tolerate in these products before they opt for something simpler (e.g., PROFS and All-in-1 were displaced by cc:Mail and Microsoft Mail).
- There is strong interest in integration with wireless handheld devices and there is much innovation in this field. Valid unified messaging offerings for widespread enterprise use will need to do a better job than most of the current offerings of data protection, integration of the “other” voicemail and email queues in an individual’s life, and integration with the enterprise directory.
- One reason why vendors are migrating to open standards wherever they can is because the integration efforts are thus reduced. Unless people can exchange messages freely and reliably, without barriers in addressing and attachment handling, they cannot build additional functions on top of the base.

Issues

- Standards for some groupware features are still at early stages of development (e.g., document management, forms routing).
- The ability to deploy a user or mobile unit without wires, with secure connection to the nearest satellite, is an important capability for many enterprises, as it is for Defense. Transportation, mining and drilling operations, police action, and journalism all share this requirement.

Relevant Standards and Protocols

- The IETF has released the specification for vCard version 3. The two parts of the definition are:
 - RFC 2425: MIME Content-Type for Directory Information
 - RFC 2426: vCard MIME Directory Profile
- The IESG has approved the specification for iCalendar as proposed standards. The three RFCs are
 - RFC 2445: Internet Calendaring and Scheduling Core Object Specification (iCalendar)
 - RFC 2446: iCalendar Transport-Independent Interoperability Protocol (iTIP): Scheduling Events, BusyTime, To-dos and Journal Entries

- . RFC 2447: iCalendar Message-based Interoperability Protocol (iMIP)
- . ISO 8601: The international standard for representation of dates and times.

Direct Answer

- Groupware features (e.g., scheduling, newsgroups, document sharing) will continue to be integrated with traditional COTS electronic mail and are essential to a robust messaging system.
 - Groupware features will continue to modularize, permitting deployment for only those groups requiring a function in an enterprise, and permitting ASP deployment for situations requiring groupware among enterprises or connecting random users on the Internet.
6. To what extent are changes to electronic mail benefiting the portable, low throughput market segment?
- We interpret this to mean support of devices (laptops, PDAs, wireless devices) connecting over slow or limited bandwidth links (e.g., satellite). Messaging protocols such as POP and IMAP are engineered to work satisfactorily over slower links. POP provides simple pick-up and delivery with minimal dialogue. IMAP allows the user to preview the list of messages in queue for pickup and select only those messages desired in this transmission. In addition, there are advances in compression techniques and digest-preparation (e.g., Amika) that can prepare a brief digest of the message for a wireless user, with optional access to the full message if desired.
 - Mass Access Devices include the multiplicity of "toys" (hand-held devices, telephones, etc.) as well as kiosks, internet cafes, and Web TV users. These will be prevalent, like public telephones. This scenario brings about key issues including how to authenticate the user. There are provisions for telephone authentication of a user today which may serve as a model for a data analog to this process.

Direct Answer

Generally, there are few changes to email systems that are specifically benefiting portable devices connected through slow bandwidth links. Nevertheless, there is major interest in connecting such devices to corporate messaging systems and such connectivity will be widespread. Advances in technology such as WAP and faster wireless links will further stimulate the process. By 2005, half of all corporate users will be able to connect with their corporate email system using a wearable, wireless device.

7. Except for SMTP/MIME and X.400, do viable alternatives for providing messaging capabilities exist? How likely is it that these alternatives will capture significant market share?

Trends

- Instant messaging is not yet standardized and has none of the security features that are inherent in S/MIME. The standard for instant messaging, IMPP, is nearing agreement and will be implemented over the next two years. This segment is young enough that these changes should be deployed rapidly. However, this provides only best-efforts one-shot transmission of messages. If the transmission fails for any reason it is not retried.

- There are messaging middleware systems of protocols, sometimes called "Business Quality Messaging" or "BQM". Messaging middleware provides for reliable program-to-program communications (guaranteed sequence of delivery, once and only once, within a specified time, etc.). This is implemented as a separate store-and-forward infrastructure parallel with but separate from SMTP. While this is significantly more reliable than SMTP messaging, and is the preferred mechanism for inter-process communications, it will not be sufficiently widely deployed to offer an alternative to SMTP.
Nevertheless, specific groups of organizations are likely to mutually agree to use messaging middleware technologies and products to exchange information reliably. For example, two firms that work together might bilaterally agree to use BQM or another messaging middleware transport (similar to traditional bilateral agreements to use a common Value Added Network (VAN) for secure messaging.
- We see no other viable alternatives with this level of robustness and security on the horizon.

Issues

- There are no current industry efforts to turn instant messaging into a secure service. It has other goals in life – it will become an adjunct to telephony sooner than a replacement for store-and-forward email, but mail will fail over to store-and-forward messaging.

Relevant Standards and Protocols

- Same as 1 above and 8 and 9 below.

Direct Answer

- There are no viable commercial alternatives to secure SMTP/MIME.

Message Security

8. What security mechanisms will business and industry employ to secure electronic mail systems over the next 2 years?

Trends

- Within an enterprise, data protection from site to site will be handled at as low a level as possible, for simplicity of installation and use. Data protected from point to point in a network is easier to deploy than security requiring human action on a per-message basis.
- Between enterprises (B2B), messaging transfers using site-to-site encryption will be used for simplicity of implementation and use (all message between this enterprise and its attorney must go encrypted). This can be handled by the messaging servers without human action on a per-message basis.
- SSL and message staging will be used, especially when interacting with a customer with whom there is no established relationship, or when this may be the only transaction with this user (e.g., products from Tumbleweed, Click2Send, etc.).

- ASP services such as Netdox, UPS, will provide an outsourced PKI and S/MIME encrypted document service.
- S/MIME v3 using X.509 certificates for digital signing and encryption will gather momentum as public key infrastructures are deployed.
- Implementing PKI(s) with X.509 will be the primary bottleneck.
- Certificates using dual keys (one set for digital signing, another set for encryption) and escrowing of the encrypting key will become common practice.
- Biometric authentication will be introduced but not widespread.
- Use of (multipurpose) smart cards to contain authentication implementations (biometrics, private keys, etc.) will increase.
- Use of portable telephones containing private keys may become popular. These devices will connect to other devices using a standard infrared connection. They will provide a means of authenticating users. Technology in this area is evolving at a very fast pace in a race to meet the challenges of secure communications, authentication and location of users, and efficient data access (directories, stock quotes, sports scores, weather, news).

Issues

- The Transport Layer Security (TLS) for SMTP messaging and the use of secure TCP ports (in addition to the well-known TCP ports) have not been widely adopted.
- S/MIME interoperability is a key issue.
- Current lack of a production-level PKI including CAs, means of certificate distribution, and certificate repositories continues to hamper deployment of secure messaging.
- Lack of interoperability among PKI/CA providers is a key stumbling block.
- Lack of a means to establish mutual trust and certificate validation among PKI/CA providers is a key outstanding issue. This includes such legal issues as cross certification liability.
- It is very hard to check that a certificate is still valid. Online Certificate Checking Protocol (OCSP) seems to be the way the industry is going, although it will need further refinement. Inadequate certificate validity checking is a key outstanding issue.
- S/MIME v2 requires the use of RSA key exchange, which is encumbered by U.S. patents held by RSA Data Security, Inc. (should change in September 2000 when RSA's patent expires).
- S/MIME v2 requires the use of weak cryptography (40-bit keys).
- Lack of processing power to handle biometrics will hamper deployment of this technology.

Relevant Standards and Protocols

- RFC 2246: Transport Layer Security (TLS) Protocol.
- RFC 2311: S/MIME Version 2 Message Specification.
- RFC 2312: S/MIME Version 2 Certificate Handling.
- RFC 2313: PKCS #1: RSA Encryption Version 1.5.
- RFC 2314: PKCS #10: Certification Request Syntax Version 1.5.
- RFC 2315: PKCS #7: Cryptographic Message Syntax Version 1.5.

- RFC 22268: Description of the RC2 Encryption Algorithm.
- X500: ITU/ISO Recommendation X.500 – Information technology – Open Systems Interconnection – The directory: Overview of concepts, models, and services . November 1993.
- X509: ITU/ISO Recommendation X.509 – Information technology – Open Systems Interconnection – The directory: Authentication framework . November 1993.
- X509a: ITU/ISO Final text of draft amendments to X.500 | 9594 for certificate extensions. 1996.
- RFC 1847: Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted.
- RFC 1321: MD5 Message-Digest Algorithm.
- RFC 2144: CAST-128 Encryption Algorithm.
- RFC 2268: Description of the RC2 Encryption Algorithm.

Direct Answer:

- Business and industry will be nudged into using S/MIME over the next three years.
- See additions to “Trends” above

9. When are S/MIME v3 products expected to be available? How long until it will be fully deployed? When will ESS start to take off?

Trends

- The trend is toward S/MIME v2 deployment in year 2000.
- Microsoft, Lotus and Netscape have announced that support for V3 will be available in the year 2000.
- Other companies have privately so announced according to the chair of the IETF-sanctioned S/MIME Working Group.
- The adoption of ESS will depend upon the adoption of standardized labeling methods. Work is ongoing within ISO to document a standard security label, but there is no guarantee that the market will embrace it. Commercial adoption of ESS is uncertain within the next two years.

Issues

- Most network managers/email administrators are still not knowledgeable about S/MIME and version options.
- Current lack of a production-level PKI including CAs, means of certificate distribution, and certificate repositories continues to hamper deployment of secure messaging.
- Lack of interoperability among PKI/CA providers is a key stumbling block.
- Lack of a means to establish mutual trust and certificate validation among PKI/CA providers is a key outstanding issue. This includes such legal issues as cross certification liability.
- A PKI with mutual certifications of CAs is essential for S/MIME v3 to take off.

Relevant Standards and Protocols

The S/MIME v3 standard consists of five parts:

- RFC 2630: Cryptographic Message Syntax.
- RFC 2633: S/MIME Version 3 Message Specification.
- RFC 2632: S/MIME Version 3 Certificate Handling.
- RFC 2631: Diffie-Hellman Key Agreement Method.
- RFC 2634: Enhanced Security Services for S/MIME (Proposed) is a set of extensions to S/MIME to allow signed receipts, security labels, and secure mailing lists. The first two of these extensions will work with either S/MIME v2 or S/MIME v3; secure mailing lists will only work with S/MIME v3.

Direct Answer

- S/MIME V3 products will continue to appear this year, 2000.
- Deployment should pick up in 2001 through 2002.
- Full deployment will not occur before 2003.

OTHER INFORMATION

The following information may be useful for the report.

S/MIME v3 was made a standard in July, 1999. The charter for the IETF's S/MIME Working Group states that the purpose of the group is to create S/MIME v3 protocols that can become IETF standards.

Mandatory Features of S/MIME v3

Message format	Binary, based on CMS
Certificate format	Binary, based on X.509v3
Symmetric encryption algorithm	TripleDES (DES EDE3 CBC)
Signature algorithm	Diffie-Hellman (X9.42) with DSS
Hash algorithm	SHA-1
MIME encapsulation of signed data	Choice of multipart/signed or CMS format
MIME encapsulation of encrypted data	application/pkcs7-mime

X.509 PKI Characteristics		
	<i>Versions 1 & 2</i>	<i>Version 3</i>
<i>Certificate information</i>	X.500 names only. Includes CA & subject names, subject public key, and a validity period.	Fully extensible, can include any information.
<i>CA arrangement</i>	No mandated CA arrangement, however the general hierarchy with cross-certificates is encouraged. No trust constraint mechanisms.	Trust constraint mechanisms are provided. The general hierarchy with cross-certification is still encouraged.
<i>CA <-> Subject <-> User relationship</i>	CAs, subject and users are distinct.	
<i>CA<-> Subject <-> User trust relationships</i>	Each user is expected to fully trust at least one CA. CAs have no mechanism for manipulating their trust relationships with subjects and	Each user is expected to fully trust at least one CA. CAs can constrain how their trust in subjects and other CAs is

	other CAs.	delegated.
<i>Certificate validation method</i>	Offline. Certificate chains are stored locally and / or transmitted with every message. Validation is performed by checking the validity period of each certificate and verifying that the certificate does not appear on the latest available CRL.	Offline, but can be online through yet-to-be-defined extensions.
<i>Certificate revocation method</i>	Simple CRLs only.	Sophisticated CRL mechanisms. Online methods can be defined via extensions.
<i>Identity vs. credential certificates</i>	Identity certificates only. Credentials may be attached to the named X.500 directory entry.	Mainly identity certificates. Certain standard extensions provide some credential-like functionality. Can be extended to provide full credential certification.
<i>Irrefutability and strong authentication</i>	Authentication strength based on the accuracy of X.500 entries. CA is responsible for issuing certificates that are not misleading.	CA is still responsible for certificate accuracy, but use of non-X.500 names may make this more difficult.
<i>In-band vs. out-of-band authentication</i>	Users must obtain at least one CA key out-of-band. Also, the extensive use of OIDs requires out-of-band communication whenever a new extension is defined.	
<i>Anonymity</i>	Anonymous only to the degree that an X.500 entry can be anonymous.	Extensions can be used to provide fully anonymous service.

Directory

Directory Services

10. What technologies and architectures will business and industry employ to build high performance, robust, and reliable directory systems over the next 2 years?

The dominant technology for directory services over the next two years will be based on version 3 of the Lightweight Directory Access Protocol (LDAP). Vendors will have extensive deployments of LDAP servers with proprietary server to server protocols providing X.500-like protocols between servers (similar to DSP and DISP). At the same time, the X.500 standards process will likely approve extensions this summer that map X.500 protocols onto TCP/IP.

There are four simultaneous approaches occurring in the directory market:

- General Purpose Directory delivered by a variety of suppliers from X.500 to LDAP to traditional NOS vendors such as Novell. Microsoft is conspicuously missing from this group at this time, except as they deliver the MetaDirectories using recently acquired Zoomit technologies.
- Directory Enabled Networks Directory Enabled Networks will be a theme within the network infrastructure. Companies such as Cisco and Novell have announced products based on the DEN specification that support network equipment from Cisco, 3Com and Nortel Networks. The Cisco product will run using Active Directory, while the Novell product will use Novell's NDS. It is not a long stretch to expect DEN-enabled schema definitions to be supported on the iPlanet Directory Server (formerly known as the Netscape Directory Server).
- Microsoft Active Directory – initially focused on the operating system, printers, and network naming and addressing (DNS and DHCP). Microsoft plans to evolve Active Directory into a general-purpose directory and support DEN. Over the next two years there will be a significant deployment of Microsoft Active Directory as companies upgrade their current environments to Windows 2000.
- X.500 – Relative market adoption will decrease over the next 1 to 3 years, with sales remain steady due to the PKI requirements of directory servers communicating between themselves. At some point new standards will emerge and X.500 will migrate to IETF specified protocols, becoming just another LDAP server.

Timing

General Purpose is zero to three years. Active Directory early adopters in 2000, most companies will start in 2001 through 2002, with widespread deployment of Active Directory by the end of 2002. First products with deployable DEN capabilities are likely to enter the market in 2001. Early releases will only support a small subset of network equipment needed in an enterprise. Widespread usage will take 3 to 5 years. Over time, as all three of these approaches stabilize and mature there will be a convergence point no sooner than 5 years from now.

Protocols and Technical Trends and Issues

X.500 will continue to extend the current standards to encompass requirements from LDAP and Internet based directories. These standards will enhance and contribute to the overall evolution of the LDAP and Internet based standards.

Three forces of technical trends exist – X.500, LDAP and RDBMS, and will continue to be important and widely deployed technologies over the next 3 to 5 years. Each of them has different needs and requirements.

- X.500 – Design Goals focus on security and large distributed environments, often crossing international boundaries. The specifications are significantly more detailed resulting in more

complete product designs, resulting in significant interoperability capabilities because they are less ambiguous and more thorough.

- LDAP – Design goals for LDAP are high performance geared towards a single server solution solving a single specific problem, enabling rapid application development and deployment. This is typically achieved by lightweight definitions of the protocols. LDAP is often used as a standard interface to a proprietary solution.
- RDBMS – The design goal for RDBMS is to have a relational database capable of storing many different types of data. However, it is not targeted at common access controls, distribution of data amongst multiple servers, or common authentication mechanisms. It is also not designed for high performance and massive simultaneous access from a global standpoint.

Barriers to Convergence

LDAP technical issues

- LDUP – The X.500 standards process found that during the development of X.525 (ISO 9594-9) replication protocols that there are very serious considerations in building a robust and complete protocol to support the functionality between all servers and operational situations. The LDUP protocol does not address many issues that could potentially make it very difficult for very large and distributed directories. For example, LDAP schema is not enforced between replication partners, which could result in inconsistent behavior. Probably the most serious concern would be the enforcement of access control policies during the replication process.
- Chained operations – LDAP currently does not have a server-to-server protocol. A number of vendors have implemented proprietary protocols, such as Microsoft and Novell. In addition, other vendors have implemented a referral mechanism that lets the system administrator configure a set of LDAP servers from the same vendor that accept a level of trust between each other and handle the referral on behalf of the client application.
- Knowledge of other LDAP servers – there currently isn't a mechanism that lets LDAP servers build a knowledge of the distribution of naming contexts. This is not an issue for small deployments, but is a barrier to deployment for large systems.

Common Access Control – LDAP will have significant difficulty in deployments that have multiple vendor products working within a single infrastructure because of the lack of a single common access control mechanism. This will be a strong limiting factor for users who want to deploy multi-vendor environments.

PKI – Directory is the mechanism of choice for storing public keys. This trend will continue. Bridged CA's will continue to use X.500 to simplify the interoperability between different directories used by individual CA's.

Alternatives to LDAP and X.500

The only alternatives currently evolving are products that are categorized as MetaDirectory. Initially, most MetaDirectory products focus on synchronizing information between sources. This is typically an asynchronous operation that occurs at scheduled intervals, often set to 24 hours. However, there is a different approach that is beginning to make headway from vendors, namely Microsoft (with its Zoomit acquisition), Novell and ISOCOR (Critical Path). This approach creates a live connection to one or more databases and makes the data appear transparently as part of a larger directory infrastructure. Oracle is also in this product space with an LDAP interface into Oracle databases, but it is not currently targeted towards large directory deployments.

Replication Protocols – LDUP and DISP

It is unclear at this time whether or not LDUP will succeed. The issue is that the majority of LDAP server products have interoperability and conformance issues that would make it difficult to deploy. In addition, most vendors are adding custom extensions to their products to differentiate themselves. These extensions make it questionable whether or not LDUP will interoperate between vendors. Significantly, there exist serious concerns on the scalability of LDUP in very large environments.

If the interoperability is solved, there will be a serious technical issue to deal with. The mechanism that LDUP uses appears to have the capacity of generating very large messages due to the lack of encoding rules.

DOP – Directories Operational Protocol

There continues to be strong resistance from X.500 vendors in the implementation of DOP. It is unlikely that this position will change in the next two years. Each system will be required to manually configure its shadowing agreements. However, each system will typically have a Web interface that can be accessed remotely to execute the shadowing agreement. In effect, you will have two windows open, one window for each side of the shadowing agreement. Vendors will solve this in a proprietary manner for the foreseeable future.

Directory Security

11. What security mechanisms will business and industry employ to secure public and private directory systems over the next 2 years?

Security mechanisms within industry are continuing to slowly evolve and directory is part of that picture. Over the next two years, industry will continue to struggle to come to a common approach for securing public and private directory systems. Pressure will continue to grow the deployment of PKI. Strong issues surrounding the “bridging” of CAs. The attempts within the United States Federal Government will prove the concept of Bridged CA throughout the year 2000 with a limited number of Certificate Authority vendors. During the year 2001, vendors will respond to industry pressure to work together.

For industry-wide acceptance, it will have to be possible to validate a certificate with any trading partner. The current method of maintaining Certificate Revocation Lists does not easily scale to a global scale, however it remains a strong contender on management of revoked certificates. It is envisioned that industry will use the Online Certificate Status Protocol (OCSP) as a simple and deployable mechanism to validate a certificate with any CA around the world. To accomplish this, it is anticipated that OCSP interfaces to solutions like the Bridged CA will be necessary.

These OCSP interfaces will become commonplace, and commercial services will become available that will offer outsourcing of this capability. Due to the tremendous traffic that can be generated and the potentially significant processing and referrals behind the OCSP interface, it is envisioned that many commercial service offerings will use messaging middleware to permit queuing of the OCSP request.

12. Will access control be implemented from the end-system perspective (i.e., using TLS to encrypt transport layer using the workstation's certificate plus passwords over top of that to identify the specific user) or from a user perspective (i.e., using the user's certificate when doing the encryption)?

The adoption of TLS within the LDAP community is still some time off. Internet Drafts are currently circulating that define this capability. Most LDAP based products support SSL at this time, but the majority of applications currently do not use it. The X.500 standards effort is currently transitioning

its OSI seven layer protocol stack to the direct use of TCP/IP. This will make the adoption of TLS very quick by the X.500 vendors. The visibility of security is rapidly rising within industry and companies are beginning to look at what it would take to deploy PKI internally.

A larger problem is the lack of a common access control mechanism within the LDAP community. X.500 enjoys the ability of sharing access control mechanism amongst all of the vendors, yet LDAP does not have such a luxury. Every major LDAP directory employs a proprietary mechanism, which makes operations, such as replication not possible, since one product may not understand another products access control rules.

13. When will the access control be designed to support more than just ACLs (e.g., RBAC)? How widespread are non-ACL based access control schemes likely to be in COTS products?

Role-Based Access Control is currently available on a proprietary basis from most LDAP directory vendors. It is expected that the IETF process will evolve access control mechanisms that support RBAC in a standardized method. However, this will continue to be problematic on a large scale within the LDAP environment since there is no server to server protocol on the horizon which would let servers authenticate and establish a level of trust between them. Thus, a user authenticating on one LDAP server, trying to execute a referral to another server, may not be known or trusted on that remote server.

It is expected that RBAC will be common in COTS products in the future.

Security

Public Key Infrastructure

Certificate Generation

14. Is industry moving to support more than just what's in PKIX? Are they using a template-based approach (i.e., pick any of the fields required by policy and then generate them accordingly)?

The PKIX profile (RFC-2459) is too general to be useful in itself, though it is now the basis of most profiling efforts. RFC-2459 was created to meet the requirements of many diverse communities, and as such, still requires further definition with respect to several certificate extensions. The Federal PKI Technical Working Group has created a Federal Certificate and CRL Profile based on RFC-2459 (TWG-99-01; format updated in draft TWG-00-01). Additionally, the newly formed PKI Forum will use RFC-2459 as the basis for its profile. A grand vision is to have a single profile that can be demonstrated to meet the needs of the Federal PKI, the PKI Forum, and the DoD PKI 2002 (Capability Increment 1 of the DoD Target PKI).

The IETF Simple PKI (SPKI) Working Group has developed a standard form for digital certificates whose main purpose is authorization rather than authentication. These structures bind either names or explicit authorizations to keys or other objects. The SPKI concepts are documented in RFCs 2692 and 2693. These specifications have not met with wide acceptance.

15. What proprietary certificate and CRL extensions do DMS implementations need to worry about? Are there any that must be included to achieve interoperability?

The Netscape netscape-cert-type private extension is required for client authentication in Netscape Navigator 3.x clients. It has been replaced by the X.509 extensions Extended Key Usage and Basic Constraints in later products. If DMS deems it necessary to support Netscape 3.x clients, the netscape-cert-type extension should be included as required (see the Netscape Certificate Management System Installation and Deployment Guide). Otherwise, no private or proprietary extensions have been identified to achieve interoperability.

Interoperability

16. What support will be available for mixed DSA/RSA certificate path building? If DMS uses DSA and industry uses RSA, then products must support verifying RSA and DSA signatures.

It is expected that applications will adopt the processing of both the RSA and DSA signatures. However, the ability to validate paths using mixed algorithms will appear only after applications implement robust certification path validation. Because it will still be some time before applications provide this robust validation, it is questionable whether mixed algorithms will be addressed within the next two years.

The banking industry is converging on the use of RSA as defined in X9.31, and X9.31 has been added to the draft FIPS-186-2. Additionally, application vendors have stated that they will implement X9.31. It should be noted that RSA based on X9.31 is *not* interoperable with RSA based on PKCS #1, the de facto RSA standard. It is recommended that DMS consider the generation of signatures based on X9.31.

17. What support will be available for different algorithm parameters in certificate path? Not everyone will use parameters generated by NSA, if the signer does not support the same parameters verification software must support parameter inheritance.

Client applications that perform certification path validation and are able to process DSA signatures should be able to utilize differing sets of algorithm parameters within a certification path. DMS *does not* require a single set of parameters throughout the certification path (SDN.706, Appendix A). Thus, it is possible to meet the Microsoft requirement.

In general, the RSA algorithm does not require the distribution of algorithm parameters. For DSA, those parameters can be distributed in the CA certificate. (Several years ago, a substitution threat was identified on the DSA parameters that was resolved by including a hash of the next set of parameters in the current certificate.) If Elliptic Curve DSA is used in the future, there will be parameters that must be distributed for that algorithm (via the CA certificate).

Example implementation: The USPS CA currently signs all certificates using DSA even if the certificate contains an RSA public key. This means that any entity needing to use and verify the certificate must implement both DSA and RSA.

18. Will implementations widely support the scenario in which signers and recipients have more than one certificate (e.g., different roles). Netscape appears to support the recipient having more than one certificate only if they also have different email addresses.

Yes, at least it is clear that this is a real requirement for the long term as organizations move toward multiple security level architectures, with communities of interest and people who belong to multiple communities. Most of the PKI digital signature validity today surrounds one signature for one entity to meet the requirements of non-repudiation, authentication, etc. However, supporting multiple personalities based on job function would probably create a more difficult administration problem. There are two ways to look at this requirement – one is for certificates based on function being performed (e.g., signature, confidentiality) and one is for certificates based on role or community of interest.

Another reason for multiple certificates is that many organizations will issue their own certificates to avoid having to trust other certificates. Users may end up with certificate wallets.

Role-based authority is quite complicated, in that it normally involves shared authority between several individuals. As an example, General Smith may hold the role of "Base Commander" . However, there will be several aides, secretaries, etc. who are authorized to read messages addressed to the Base Commander. There will be a smaller set, including General Smith, which are allowed to sign messages from the Base Commander. These complexities result from the structure and operational requirements of military organizations. In the commercial sector there will be much less requirement for this capability. Departments such as Public Relations and Human Resources will likely have somewhat similar requirements, but will solve them through more traditional means (rather than X.509-base certificates).

The Canadian Department of National Defence Military Message Handling System (MMHS) will utilize Entrust Technologies for their cryptosystem, and has significant role-based authentication and signature requirements. It will begin deployment in late 2001, and will likely be the first major system to attempt to implement role-based authorization and signatures. Their approach will be implemented in the directory and messaging user agent technology, not as a feature of the PKI itself.

As credit cards adopt smartcard and PKI technologies, it is quite easy to envision that a single individual may have a dozen or more "identities" which are allocated to everything from their site access control card to their personal VISA card. An evolving model which may become useful in the 3-5 year timeframe is based on current credit card authorization services. Currently, these services not only validate that the card is active and has sufficient credit left, but also can approve specific types of purchases (e.g. hotels are ok, bar tabs are not allowed). Extensions to these services could provide role or functional authorization as well, based on the identity of the person holding the credentials.

DMS Fortezza currently supports multiple roles, with multiple certificates per user, but each has a different directory entry.

Entrust implementation – More than one account can be created for each person; the software treats the multiple accounts as distinct entities.

Microsoft Outlook 2000 - Already supports multiple certificates (one for authentication and one for confidentiality). Because this is a feature sought throughout the PKI market, additional applications are expected to support multiple certificates.

In the 3-5 year timeframe, experience with various early systems may lead to directory-based methods of aggregating the various certificates and permissions into a single entry (e.g. a "digital wallet" with authorizations). Commercial requirements flowing from electronic commerce initiatives will generate offerings which will perform role-based authorization as part of certificate validation services.

19. Is support for different certificate policies being implemented? Future DMS implementations are expected to support multiple certificate policies and implementations will need to allow the user to pick the certificate accordingly.

The Certificate Policies extension is not widely supported by commercial applications. There are a number of issues that are not addressed within X.509 that may inhibit the commercial acceptance of certificate policies. For example, there is not a standard mechanism to indicate the assurance that a particular transaction requires; certificate policies are currently associated with certificates (Certificate Policies extension) and with applications (initial-policy-set), but not individual transactions. Additionally, if a transaction requires Medium Assurance (Class 3) signature, is it acceptable for the transaction to be signed with a High Assurance (Class 4) certificate? If so, there is not standard way to convey this; this may be accomplished by including multiple certificate policies in the certificate (Class 2, Class 3, and Class 4), or by including a similar set of certificate policies in the initial-policy-set associated with the application. Either solution can work, but both have different results, and all communicating parties must agree on the same approach. Thus, until the concepts associated with certificate policies is fully developed, the commercial market will be slow to accept them. In the near term, this is being addressed by using multiple points of trust where each point of trust represents a certificate policy domain.

On a side note, physical identification of users may be required to issue the certificates, such as in person visit, passport, other id. Also need to consider what policy means with respect to different sensitivity levels. Will issuance authorization vary depending on the sensitivity level?

Within military systems, certificate policies determine a person's right to create or access information of specific security classifications. Since the usage and distribution of that information assumes that it was marked correctly at creation, ensuring the identity and authorization of the user is paramount. These authorizations are typically based on the identity of the individual.

In commercial environments, there exists much less requirement to grant a level of authorization to a user. Authority typically relates to the job function (e.g. allowed to sign Accounts Payable checks, but not Payroll checks), or to the asset being accessed such as a door-key, safe, or network sign-on. In these cases, the identity of the individual could be proven using a smartcard-based certificate, but the policy of what can or cannot be access would probably be maintained centrally – not with the cert.

It is unlikely that commercial offerings will ever meet the military's operational and security requirements for certificate policies. It may, however, be possible to provide major vendors with a better understanding of these requirements so that future products could more easily accommodate these requirements. If these requirements can be linked to future business, this may provide a sufficient business case to encourage vendors to accommodate the government's needs.

Certificate Revocation

20. To what extent will implementations 2 years from now support "late verification"? This refers to the scenario in which an implementation must verify a dated signed object using a certificate that was invalidated, but which was valid at the time the signature was applied. In other words, the signature was good when the object was originally received but time has passed and the certificate (for whatever reason) has expired or been revoked. Will the signature still be considered to be valid?

The ability to support "late verification" is related to the ability to support an archive capability. Through an archive, complete certification paths and CRLs must be stored and managed to enable future certificate validations of current signed objects.

Some products (such as Entrust and RSA) are supporting "key histories" – the ability to associate an old key pair with the data that was encrypted by that key pair – not sure how similar support will be provided for signatures, but this should also be possible with these products.

The archive feature to date has been a theoretical exercise. Much effort will need to be focused on this archive requirement to implement this feature within the next two years.

21. When MISSI initially looked at supporting the different types of CRLs, there was no industry support for Indirect CRLs (ICRLs) or delta CRLs. Should DMS investigate support delta CRLs?

DMS should execute an in-depth analysis of the various options related to revocation. There are a wide variety of options, including numerous concepts with respect to CRLs, as well as Online Certificate Status Protocol (OCSP). DMS should determine the most efficient and most effective method for implementing certificate revocation for its community. Indirect CRLs, partitioned CRLs, and Delta CRLs are several of the options with respect to CRLs. Few products implement CRLs, let alone the sophisticated variations described here. Entrust and RSA implement CRLs within their own trust hierarchy. This should be available in the next 2 years more widely. Short term delta CRLs are most likely to be implemented but don't scale well as the system grows. Somehow an improved flavor of OCSP will be important.

22. Will interoperable OCSP implementations be available in the next two years to support online certificate verification?

OCSP implementations are already coming to market. Within the next two years, products implementing this protocol will continue to emerge. Valicert is currently offering this as a product, both as an OCSP responder and an enhancement for the certificate processing application. Verisign is also a proponent of this standard. We expect to see more toolkits enabling OCSP implementation. And it should be a feature in mid-term commercial applications. As a side note, ValiCert is saying that OCSP is inadequate and will need further development; if true, this may delay the timing for a commercially-useable OCSP across the community.

23. Are SCVP servers (off-loading certificate verification to a server) being seriously considered by industry?

SCVP servers are seriously being considered by industry. This enables the implementation of the "light client," allowing a less expensive and less resource-dependent client implementation. OCSP is a principal component of this concept.

Beyond certification validation, there are also concepts of utilizing OCSP to validate the *authorizations* of clients to access enterprise servers. This may be executed by a validation server performing both certificate and authorization validation.

24. Are there other revocation technologies being developed that will be deployed in the next two years?

The Certificate Suspension List (CSL) is a current topic, however it has not met with widespread interest. The CSL enables a certificate to be temporarily suspended until either the suspension is revoked or until the certificate is revoked. There is no current indication that this will become adopted within industry. Thus, CRLs and OCSP continue to be the only foreseeable revocation options.

Attribute Certificates

25. How far along are attribute certificate (AC) implementations?

Attribute certificate implementations are not very mature. The only promise of a commercial product has been by Baltimore Technologies, and their product will not be available commercially for some time. Additionally, if a commercial *attribute authority* were available, no commercial applications are prepared to use them and no commercial toolkits are available.

The X.509 standard continues to evolve with respect to attribute certificates. A Draft Amendment (DAM) to X.509 is in ballot in ISO. This would result, perhaps, in an X.509 2000. The DAM addresses many of the shortcomings with respect to attribute certificates and will be an important step forward in making attribute certificates an implementable concept. One of the principal shortfalls in the current definition of attribute certificates is the concept of trust—how do I know whether this attribute authority has the authority to issue this attribute? The DAM addresses this through the introduction of a *source of authority*.

26. Where are industry implementations moving for the trust point for the AC issuer? Is it based on implicit trust or are the AC issuer's certificate verified up to a trust point in the PKI?

The DAM to X509 addresses the point of trust through the implementation of several new extensions including, *authorityAttributeIdentifier*, *delegatorAttributeIdentifier*, *attributeDescriptor*, and *sOAIdentifier*.

Conversely, if the attribute authority is the owner of the data to be accessed, the attribute authority can be said to implicitly trust itself, and thus it needn't convey a point of trust. For example, the owner of an enterprise server containing data to be accessed may generate its own attribute certificates to implement fine-grained access control of its data to known entities. In this case, the server must maintain the list of attribute certificates only for its own use and needn't convey a point of trust.

27. What revocation schemes are likely to be supported by industry AC implementations? Will they only support short lived ACs (i.e., no AC CRLs)?

Because the concept of attribute certificates is still in its formation stage, the concept of attribute revocation is ill-defined. Attribute revocation lists (ARLs), OCSP, and short validity periods are all viable revocation concepts.

DVCS

28. Are data verification and certification servers a viable solution for supporting non-repudiation services? Will widespread, interoperable implementations be available in the next two years?

The panel is not aware of solutions in this area for non-repudiation.

Trusted Time

29. What technologies and architectures will business and industry employ to build high performance, robust, and reliable trusted time systems over the next 2 years?

Work is progressing within both ISO and IETF-PKIX to standardize the time stamp protocol. The approach within ISO Working Draft (WD) 18014 is to be compatible with the IETF PKIX working group's Time Stamp Protocol document. The IETF approach focuses on digital signatures as the means to bind information within time stamp tokens. The ISO WD takes a broader and more generic approach to accommodate the diversity of time stamp mechanisms that exist within the community. This includes the standardization of other mechanisms beyond the particular mechanisms to be standardized by the PKIX working group. To achieve interoperability between ISO and IETF proposed standards, ISO has adjusted its messages and tokens in an attempt to align as closely as possible with the IETF standard while still serving the diverse interests of the group.

With the speed at which IETF standards are completed, adopted, and implemented, we expect to see the availability of trusted time systems within the next two years.

Cryptography

30. What cryptographic algorithms are likely to be widely supported for the following in the 2-year time frame?

- Confidentiality (e.g., DES, 3DES, RC2, Blowfish, SKIPJACK)
- Key Exchange (e.g., RSA, Ephemeral-Static Diffie-Hellman, KEA, Elliptic Curves)
- Digest or Hash (e.g., MD5, SHA-1)
- Digital Signature (e.g., RSA, DSS/DSA, Elliptic Curves)

Answer:

Confidentiality – DES, 3DES, RC2, RC4 and PGP (individual and some enterprise level)

Key Exchange – RSA, KEA, Elliptic Curve

Digest/Hash – MD5, SHA-1, SHA-2

Signature – RSA, DSA, DSA-2, Elliptic Curve

Note that Europeans seem to prefer IDEA – International Data Encryption Algorithm.

RC4 is most likely for encryption of SSLs—it is the primary SSL encryption standard now. 3DES is the likely near term winner for email. DES will still have some use. The Advanced Encryption Standard (AES) algorithm (s) is (are) expected to be selected by NIST in April 2000. Over time, it is reasonable to expect that many DES and 3DES applications will switch to AES. The SHA-1 hash algorithm will dominate new applications because RSA now favors SHA-1 over MD5. For key exchange, RSA, KEA (which is a Diffie-Hellmann), and EC will dominate. For digital signature, all three listed plus DSA-2 will be supported.

31. What effect will the RSA patent expiring later this year have on support for DSA in products?

No effect. The commercial market currently provides only limited support for applications processing DSA, and the expiration of the RSA patent will not lessen the availability of DSA-capable applications. The government is expected to let the market sort itself out and not interfere in this debate once the patent expires.

32. When the AES finalist is chosen what impact will it have on above answers?

The AES will be expected to dominate in new applications and be retrofitted into

selected existing applications. It is expected that there will be multiple algorithms approved as part of the Advanced Encryption Standard. These algorithms will be added to the list of confidentiality algorithms appearing in #36. Market forces would likely drive the selection of a de facto standard over time. Some product vendors are already working to incorporate the five algorithm finalists. The five finalists include RC6, 2-fish, IBM MARS, Serpent, and Rijndael (Belgium). Final decision is expected within 18 months and it is likely that at least one U.S.-based algorithm and one foreign algorithm will dominate.

33. What cryptographic tokens are likely to dominate in the 2-year time frame? What are their primary characteristics?

- Processing Speed
- Certificate and Key Storage
- Interface Specifications

Smart cards are the most likely candidate to dominate in the cryptographic token market in the 2-year time frame. Also, smart cards will develop in the commercial world as multifunctional devices used for access, card swiping, credit/debit purchases, etc.

For all online financial transactions, speed is the most important requirement. There are two reasons for speed being important the first is that companies are paid by the number of transactions they process. The second is that transactions not returned within a certain period of time cause reversal initialization, which can cause problems with reconciliation and systemic processing slowdowns. That said, the biggest issue will not likely be processing speed or storage on smart cards – both are adequate and growing as technology advances. The biggest issue will be the interface to applications. There are so many APIs and special adapters right now. The battle will be between the smart card vendors who already have their interface standards defined and some of the computing giants such as Microsoft with their own API formats. Not clear which camp, if either, will emerge victorious in the standards area.

Appendix C: General Industry Trends

Introduction

E-business transformation skyrocketed in 1999. Various sources predict that the market will increase from \$50 billion in 1998 to \$1.3 trillion in 2003.

Key Market Drivers

- Internet
- Globalization
- Deregulation
- Customer expectations and demands increasing
- Rapid technology turn over
- 24x7x365 business
- Merger mania

Key Market Trends

- Global e-business transformation around control (customer versus supplier) and value integration
- Lower barriers to entry for competition
- Emergence of extended enterprise
- Progression of the role of IT from cost center to productivity tool to competitive advantage (corresponding focus evolving from TCO to ROI to Strategic Value)
- Transition from centralized computing to client/server to intelligent network
- Technology convergence
- Commoditization of basic email and the frenzy for competitive advantage
- Scarcity of IT resources
- Emergence of high availability, secure public networks
- New channels – ISP/ASP/ESP/WSP/RSP . . .
- Decision making and IT organizational structure is shifting from distributed to centralized. This is a pendulum-swing—it went too far toward distributed, and is coming back to more centralization (not complete centralization) in order to moderate cost and complexity.
- IT is being restructured to address new e-business requirements
- Emerging trend towards outsourcing infrastructure services
- Increasing mobility of workers, growth of the electronic workplace and of distributed workgroups
- Standardization and diversification of end-user devices, increasing popularity of smaller, hand-held devices and public Web access terminals
- Increasing requirement for authentication and data security for conducting business
- Mergers and acquisitions in Internet space
- Convergence of voice, fax, and data networking

Enterprise Problems

- Understanding and creating a framework for competing in the digital economy
- How to transition to e-business while maintaining and expanding their current business
- Scarce resources
- Continuous re-skilling and re-training
- Keeping ahead of rapid technology innovation
- Keeping up with customer demands
- Keeping pace with the competitors and market changes
- Pressure to do more with less
- Aligning technology/business/markets
- Realigning staff after Y2K
- Challenges to survive “spikes” in business activity—bandwidth, data capacity, and staffing capacity for peak times
- The challenge for most businesses is to provide value and differentiation in the face of ever increasing complexity while they aggressively pursue an e-business strategy. These companies need to deliver on traditional products, expand new and changed products, participate in newly created electronic markets and redefine what customers and markets means.
- To be successful requires strong alignment between the CEO, CIO, CFO and COO. Realizing the true value from e-business requires integration between vision, planning, development and management:

Critical Success Factors for the Enterprise

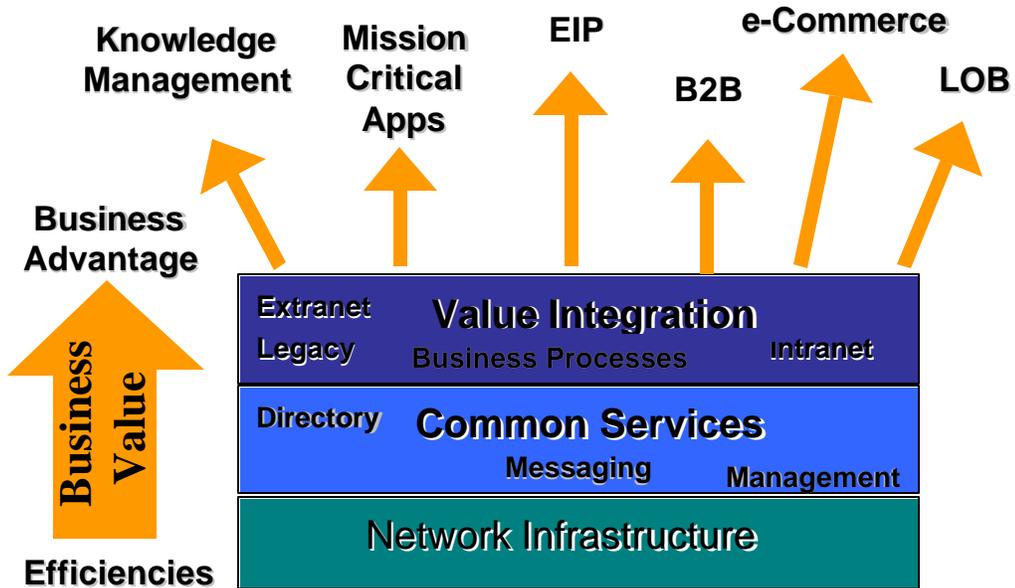
- Executive commitment
- Measure results of e-business initiatives and act on the information
- Prioritize funding and implementation by business value (not cost savings)
- Shift from decentralized to centralized development, IT/network infrastructure(?)
- Plan for flexibility, rapid change, rapid deployment of new functions
- Governance
- Integrate business strategy with technology planning and delivery from strategy to e-solutions to implementation, operations and outsourcing
- Business process integration
- Internet/extranet integration
- Back-end and infrastructure integration with new e-business solutions
- “Knowledge management” to allow the enterprise to locate, retrieve, and leverage its investments in people and knowledge
- Users and IT managers have grown accustomed to living in a dual world of communications: one part mediated by the telephone, the other by the computer. This division is disappearing fast.

- New devices and new networks will radically disrupt the architectures and assumptions underlying most enterprise communications.
- Outsourcing will be one of the least painful escape route in many cases.
- For enterprises to weather this change without massive loss of efficiency will require relearning how to focus on users needs.

Enterprise Executive Focus

The CEO, CIO, CFO and other IS/IT and Line of Business executives and managers have different concerns when approaching their company's strategy for e-business:

Decision Maker	Focus
CEO	<ul style="list-style-type: none"> • Create sustainable competitive advantage
CIO	<ul style="list-style-type: none"> • Business partnerships • Market leadership • Customer care • Reduce time to market • Shareholder equity
CFO	<ul style="list-style-type: none"> • Value chain integration • ROI • Leverageable infrastructure • Reduce costs • Rapid delivery • Knowledge transfer • Repeatable processes • Business value • Protect enterprise assets (including data) • Ensure appropriate level of security around customer information (credit cards, banking details, patient confidentiality, etc.)
IS/IT Decision Makers	<ul style="list-style-type: none"> • Rapid ROI • Measurable results • Reduce days in inventory • Reduce days in receivable • Reduce TCO • Reduce theft, bad debt
Line of Business Manager	<ul style="list-style-type: none"> • Technology • Deployment and training costs • Transition and coexistence • Cost savings • Infrastructure • Scalability/performance/ manageability • Ease of use • Application solution • Business value • Ensure sufficient elasticity of resources for peak load times



Copyright 2000, Creative Networks, Inc.

Industry Watchers Agree:

“The outsourced applications market will grow to \$21.1 billion by 2001.”

Forrester Research

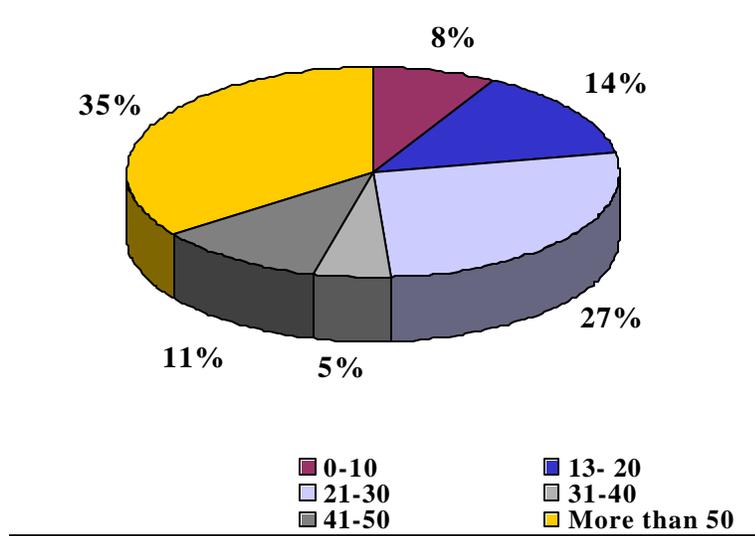
“Web-based application outsourcing will ultimately become the dominant model for how applications are delivered.”

ASP News Review

“The market is really evolving toward a mix of software and services -- not just applications but information.”

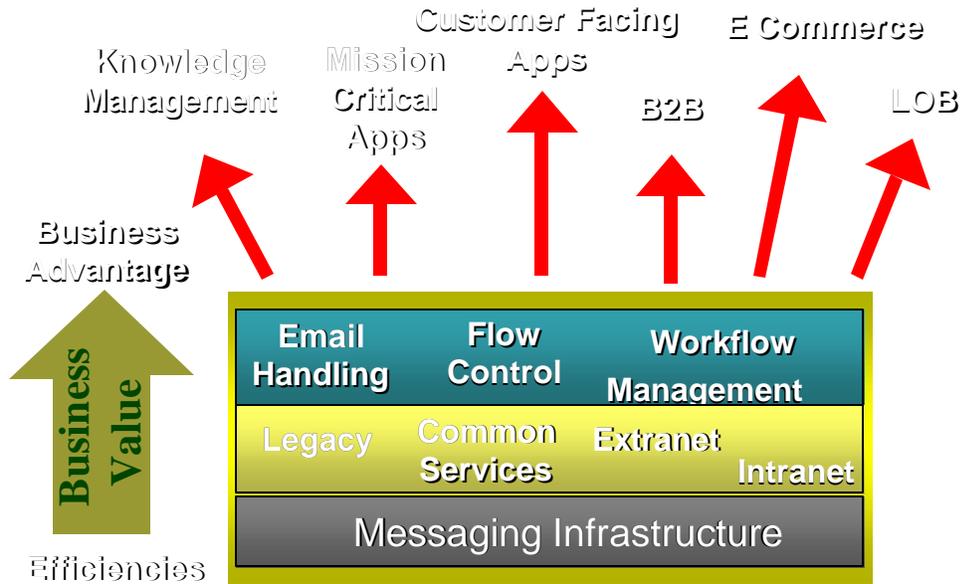
Enterprise Applications Consulting

Business Information Stored in the Email System



• Percent of Business Information Kept in the Email System

Copyright 2000, Creative Networks, Inc.



Copyright 2000, Creative Networks, Inc.

