

Secure Messaging Challenge Summary Report

Secure Messaging Challenge Team
Messaging Forum
The Open Group

June 2002



Compiled by: Dean Richardson, The Boeing Company

The Open Group ♦ Apex Plaza ♦ Forbury Road ♦ Reading, Berkshire RG1 1AX UK
Tel: +44 (0)118 950 8311 ♦ Fax: +44 (0)118 950 0110 ♦ www.opengroup.org

Table of Contents

Acknowledgements	iii
Messaging Challenge Participant Organizations	iv
1. Introduction	1
2. Scope	2
2.1 Perimeter Architecture.....	2
2.2 Internal Architecture	2
3. Testing Results	2
3.1 Testing Conditions	2
3.2 Testing Summary	3
3.2.1 Mail Servers	3
3.2.2 Mail Clients.....	3
3.2.3 Messages.....	3
3.2.4 Test Series	4
3.2.5 Test Cases.....	4
3.2.6 Statistical Summary.....	7
3.3 Challenges Encountered.....	7
3.4 Reasons for Testing Failures.....	7
3.5 Notable Achievements.....	7
4. Conclusions	7
4.1 Critical Success Factors	7
4.2 Lessons Learned	7
Appendix A: Boeing Internal Architecture	8
Appendix B: Lynx Internal Architecture	9
Appendix C: NASA Internal Architecture	10
Appendix D: smtpstbed.com Internal Architecture	11

Acknowledgements

Considerable effort went into the design, planning, and successful public demonstration of the Secure Messaging Challenge. Experts from around the world, both customers and suppliers, joined to define, create, and demonstrate the exchange of encrypted email among multiple companies using many existing standards-based applications. The Open Group and the Challenge Team would like to extend its gratitude to this dedicated group of individuals and their sponsoring companies:

Management	Dean Sepstrup, The Boeing Company
Architect	Wen Fang, The Boeing Company
Test Management	Paul Van Avery, FTT Consultants, Inc.
Marketing Director	Dean Richardson, The Boeing Company
Technical Coordinator	Russ Chung, American Eagle Group
Test Coordinators	Kermit Russell, NASA Stephan Wappler, Lynx Consulting Group Kim Warford, The Boeing Company
Demonstration Coordinators	Wen Fang, The Boeing Company Stephan Wappler, Lynx Consulting Group
Test Validators	Fred Berlack, Ferris Research Paul Evans, Booz Allen Hamilton David Ferris, Ferris Research Roger Mizumori, Waterforest Consulting Services Jonathan Penn, Giga Group
Summary Report Author	Dean Richardson, The Boeing Company
Summary Report Reviewer	Dan Blum, The Burton Group
Messaging Forum Director	Teresa Schauer, The Open Group
Messaging Forum Chair	Dean Richardson, The Boeing Company

Messaging Challenge Participant Organizations

- American Eagle Group
- The Boeing Company
- Directory Works
- FTT Consultants
- Lynx Consulting Group
- MaXware
- Microsoft
- NASA (Goddard Space Flight Center)
- solutions4networks

Active Challenge Team participants engaged in one or more of the following activities:

- Development
- Testing
- Public demonstration of the Secure Messaging Challenge in Anaheim, California

Each organization donated all labor, hardware, and software required to complete their assigned tasks.

The Challenge also maintained a mailing list and those on the list received all Challenge minutes and were able to access all Challenge material and attend Challenge teleconferences.

The Challenge Team would also like to recognize several individuals whose special contributions to the Challenge helped make it a success:

- Renée Barnow (McKinley Marketing Partners)
- Alexis Bor (DirectoryWorks)
- Brian Dilley (Booz Allen Hamilton)
- Dr. Frank Gutberlet (Lynx Consulting Group)
- Franz Mülkens (Lynx Consulting Group)
- Andreas Roscher (Lynx Consulting Group)
- Michèle Rubenstein, (solutions4networks)
- Bill Stroeing (The Boeing Company)
- Dennis Taylor (NASA—Goddard Space Flight Center)
- Brad Wright (The Boeing Company)

The following members of the Challenge Team contributed to this Technical Report:

- Wen Fang (The Boeing Company)
- Stephan Wappler (Lynx Consulting Group)
- Paul Van Avery (FTT Consultants, Inc.)

1. Introduction

Many organizations have been eagerly awaiting a way to exchange encrypted email. While many email, directory, and secure messaging standards exist, there has not been a single widely accepted method that ties these individual standards together. The need existed for creating a standard architecture for company-to-company exchange of strongly encrypted email that is both vendor neutral and relatively easy to implement and support.

Several factors hampered acceptance of previously proposed solutions:

- Proprietary, requiring using one or more specific products
- One or more third parties, requiring brokering public key information
- Bridge Certificate Authorities do not interoperate
- Manual exchange of individual end-user public encryption keys

Proprietary Software. The “proprietary software” solution is not practical as it requires and relies on purchasing a particular piece of software, which makes the entire architecture dependent on the survival of the company producing the software. In addition, because there are many providers of different proprietary solutions, most of which do not interoperate, one would need to support each and every proprietary solution to ensure the ability for everyone to communicate. This does not scale.

Third Party Broker. The “privately owned, sole authority third party key broker” solution has similar drawbacks as it requires using a master third party that every company must trust to broker key information and ensure the information is shared only with the appropriate partners. This solution also places the entire architecture’s existence in the hands of the third party providing the broker service.

Bridge Certificate Authority (CA). The “bridge CA” solution (often government implemented) seems to be gaining traction with several governments and private entities operating their own bridge CA services, but interestingly, the individual bridge CAs the Challenge Team has seen do not interoperate.

Manual Exchange. The “person-to-person key exchange” solution (most typically PGP—Pretty Good Privacy) is what most companies that require external encryption use, but this type of implementation has several disadvantages. The person-to-person solution does not scale well because each user must manually and individually exchange keys with every person to whom they wish to send or receive encrypted email. Certificates are widely available on the Internet, which creates the possibility that employees will obtain their own keys directly from the Internet, rather than from a company-owned or approved certificate server. In such a case, the company would have no way to decrypt the email if the employee loses his or her private key or if the employee quits or is terminated; therefore, all encrypted data would be lost.

Faced with the above deficiencies in existing methods, the Challenge Team made its goal designing an architecture and standard methodology for exchanging encrypted email between companies. The architecture had to be supplier neutral and standards based to eliminate reliance on or requirement for any one product, supplier or service. To this end, the Challenge Team believed it was best to make the internal architectures of each company out of scope of the proposed standard, so while the team did provide examples of how they were able to successfully implement different internal architectures that interoperated with the Challenge perimeter architecture, many different internal configurations are possible.

2. Scope

The Challenge Team determined that the scope of the Challenge should be limited to configuration of the perimeter directory servers and use of certain industry standard protocols and conventions. This scope limitation was intentional to make the architecture as widely adoptable as possible by organizations that have already deployed messaging and directory infrastructures.

2.1 Perimeter Architecture

All perimeter directory systems had the following requirements:

- **Directory**—Each organization must provide a publicly accessible LDAP directory to support lookup of email addresses and user certificates
- **Certificates**—All certificates must be issued using X.509 v.3 CA Services. Certificates may be self-signed or commercially purchased. Certificates must use Rivest, Shamir, and Adelman (RSA) algorithm with a minimum 1024-bit key length
- **Directory Protocols**—All perimeter directories must support LDAP v.3.
- **Email**—Provide S/MIME compliant email client capable of requesting certificates from the directory. Provide S/MIME compliant email backbone and servers.
- **Schema**—
 - User certificates shall be stored in the userCertificate attribute
 - Email address shall be stored in the dn attribute
 - Username shall be stored in the cn attribute

2.2 Internal Architecture

Internal architecture must be S/MIME compliant and messaging clients must support requesting certificates from an LDAP directory. While specific internal architecture was out of scope for the Challenge, diagrams of the architectures used in the Challenge have been included as appendices for reference purposes.

3. Testing Results

The Challenge test team defined a rigorous testing environment to ensure useful, documented, and defensible testing results. Testing roles were defined in the infrastructure and applications teams, and formal test plans were developed for each of these groups. This section briefly describes the testing environment (from the Challenge Test Plan document) and summarizes the test results from infrastructure and applications.

3.1 Testing Conditions

Challenge testing addresses the application scenarios and secure messaging components environment belonging to the WEMA Security Challenge. The Test Plan assumes that other necessary components (e.g., a hardware platform and its operating system) have undergone prior testing and validation. Activities such as program execution, design specifications, debugging, or system testing are beyond the scope of Challenge testing.

The products introduced into the Challenge environment will be assumed to be production environment ready. Products labeled as "Alpha" or "Beta" versions are discouraged unless they meet the criteria cited in 2.1, Perimeter Architecture.

Testing imposed the following conditions or "rules":

1. Organizations must be members of The Open Group and must be registered Challenge participants
2. Participants bringing product, service, or components must have submitted a Technical Survey Form
3. Participants must follow Test Plan procedures
4. Testers must use the validated data provided
5. Testers (and others) may not discuss or publish results outside the Challenge prior to public demonstrations and publication of the Challenge Summary Report.

A trial run of test scenarios was conducted before documented testing began. This trial served as a "reality check" for connectivity, directory schema, and the application scenarios. Participants were *not required* to execute all tests.

For complete information about the testing and a chart of the Major Milestones, please consult the Test Plan document.

3.2 Testing Summary

3.2.1 Mail Servers

The following mail servers were used during testing:

- Microsoft Exchange 5.5 SP3
- Microsoft Exchange 2000
- Lotus Notes 5.0.8
- UNIX Sendmail
- Linux Sendmail 8.1.1

3.2.2 Mail Clients

The following mail clients were used during testing:

- Microsoft Outlook 2000 SR1 International + Security Patch*
- Microsoft Outlook 2000 SP2
- Lotus Notes 5.0.8

3.2.3 Messages

Two text messages were specified to use in testing:

- Short message (1KB)
- Long message (67KB)

While the type of attachment to be used for a specific test was specified (i.e., .doc, .xls, .jpg), the file itself was not. Testers were given an Event Log on which to record any unusual results encountered not specifically related to the test case.

*Because of the popularity of Microsoft Outlook Express and Outlook Express (International) among users, the Challenge intended to include those messaging clients to test interoperability. However, when using a digital certificate obtained or confirmed from an LDAP directory, Microsoft Outlook Express uses 40-bit encryption to send an encrypted email message rather than 128-bit encryption. According to Microsoft Tech Note Q262003, RC2 40-bit encryption is the default by design because Outlook Express cannot determine if the recipient is able to accept 128-bit encryption. Challenge testers confirmed this default behavior, and because 128-bit encryption was a Challenge requirement, Microsoft Outlook Express was not used during interoperability testing.

3.2.4 Test Series

The tests were divided into 12 series as follows:

- Series 1—Clear Text Transmission
- Series 2—Send/Receive Encrypted Mail
- Series 3—Send/Receive Signed Mail [Optional]
- Series 4—Send/Receive Signed & Encrypted Mail [Optional]
- Series 5—Delivery Receipts
- Series 6—Send/Receive/Open Encrypted Mail with Attachment
- Series 7—Send/Receive/Open Signed & Encrypted Mail with Attachment [Optional]
- Series 8—Reply to Mail with Attachment [Optional]
- Series 9—COPY TO:
- Series 10—Distribution Lists
- Series 11—CAs & Certificates
- Series 12—Directories

The test series marked as “Optional” were deemed out-of-scope for the Challenge, but participants with signing capabilities who wished to do so could perform them. If performed, the results were reported. Tests were not conducted for Series 8, 11, or 12.

3.2.5 Test Cases

Each series contained several test cases designed to demonstrate the specified capabilities of that series. For example, the Series 2 Test Cases 1-6 were as follows:

- 1 Send **Encrypted** email (short message)
- 2 Open **Encrypted** email (short message)
- 3 Confirm receipt (reply) clear text
- 4 Send **Encrypted** email (long message)
- 5 Open **Encrypted** email (long message)
- 6 Confirm receipt (reply) clear text

An example of a test case follows. And results of Series 2 are provided in the matrix on page 6.

WEMA Secure Messaging Challenge 2001

Test Series & Case Number: 2 --- 1

Client Utilized	_____
Server Utilized	_____

Target Address _____

Other Addresses:

#1 _____ #2 _____ #3 _____

Purpose or Objective

To test the capability to encrypt the message and send it.

Examiner Instructions

Send **Encrypted** email (short message).

Expected Results

The short text message is successfully encrypted and transmitted.

Examiner Comments/Observations

All examiners are encouraged to note any unusual or special results encountered during this test.

Note: If you encounter unexpected results NOT RELATED to the Test Case itself, please use the **EVENT LOG** to report it.

Reserved for Test Team Use Only

Examiner: _____

Validator: _____

Date: _____ Review Date: _____

Time: _____

Comments: _____

Test Case Series 2

Send/Receive Encrypted Mail

Case #	Case Description	Client	Server	Examiner	Validator
1	Send Encrypted email (short message)	MS Outlook 2000	MS Exchange 2000	A. Roscher	F. Berlack
1		Lotus Notes 5.0.8	Lotus Notes 5.0.8	S. Wappler	J. Penn
1		Lotus Notes 5.0.8	Lotus Notes 5.0.8	F. Gutberlet	F. Berlack
1		MS Outlook 2000 SP2	MS Exchange 5.5 SP3	K. Warford	J. Penn
2	Open Encrypted email (short message)	Lotus Notes 5.0.8	Lotus Notes 5.0.8	S. Wappler	J. Penn
2		Lotus Notes 5.0.8	Lotus Notes 5.0.8	S. Wappler	F. Berlack
2		MS Outlook 2000	MS Exchange 2000	S. Wappler	F. Berlack
2		MS Outlook 2000 SP2	MS Exchange 5.5 SP3	K. Warford	J. Penn
3	Confirm receipt (reply) clear text	MS Outlook 2000 SP2	MS Exchange 5.5 SP3	K. Warford	J. Penn
3		Lotus Notes 5.0.8	Lotus Notes 5.0.8	S. Wappler	F. Berlack
3		MS Outlook 2000	MS Exchange 2000	S. Wappler	F. Berlack
4	Send Encrypted email (long message)	Lotus Notes 5.0.8	Lotus Notes 5.0.8	S. Wappler	F. Berlack
4		Lotus Notes 5.0.8	Lotus Notes 5.0.8	S. Wappler	J. Penn
4		Lotus Notes 5.0.8	Lotus Notes 5.0.8	F. Gutberlet	F. Berlack
4		MS Outlook 2000 SP2	MS Exchange 5.5 SP3	K. Warford	J. Penn
5	Open Encrypted email (long message)	Lotus Notes 5.0.8	Lotus Notes 5.0.8	S. Wappler	F. Berlack
5	†	Lotus Notes 5.0.8	Lotus Notes 5.0.8	S. Wappler	F. Berlack
5	*	Lotus Notes 5.0.8	Lotus Notes 5.0.8	S. Wappler	F. Berlack
5		MS Outlook 2000	MS Exchange 2000	S. Wappler	F. Berlack
5		MS Outlook 2000 SP2	MS Exchange 5.5 SP3	K. Warford	J. Penn
6	Confirm receipt (reply) clear text	Lotus Notes 5.0.8	Lotus Notes 5.0.8	S. Wappler	F. Berlack
6	*	Lotus Notes 5.0.8	Lotus Notes 5.0.8	S. Wappler	F. Berlack
6		MS Outlook 2000	MS Exchange 2000	S. Wappler	F. Berlack
6		MS Outlook 2000	MS Exchange 2000	S. Wappler	F. Berlack

* The target address on this test differs from the target address on the previous test, although client and server are the same.

3.2.6 Statistical Summary

As of the publication date of this report, the following had been achieved:

- Completed tests submitted—612
- Completed tests sent to validators—487
- Validated results returned—453

3.3 Challenges Encountered

Several technical and operational challenges were encountered in preparing to conduct the Challenge test plan:

- Initial configuration of the clients for similar default encryption level required vendor released registry configuration changes
- Legal research was required prior to exchanging organizational root certificates. There were no clear guidelines concerning governmental regulation of root certificate distribution.
- Exposure of the LDAP port 390 through organizational firewalls is not yet a common practice, which introduced delays as security concerns needed to be addressed

Each of the above issues was solved prior to starting testing. As an example of an issue that changed the content of the testing, the following item was not able to be resolved:

- One optional test group could not be conducted due to difficulties in reconfiguring the CA to issues client certificates that would expire within the test period

3.4 Challenge Testing Failures

The very small number of failures the validators reported were failures on the part of the tester or the reporting process, not technology failures. There were no reported instances of a message not being delivered, not being properly decrypted, or having been corrupted in transit.

The following types of failures were reported:

- **Blank test case forms being included in a package of test results**
 - One tester initially submitted the entire Series 10 cases as blank reports. Upon further review, it was determined the enclosure was the error, not the failure of the tests.
 - Another tester included five blank test cases in a package (Tests 2-2, 2-5, 2-6, 6-12, and 10-6.) Again, it was determined this was an error of submission. The tester had not run those cases.
- **Reporting a test result on the wrong form**
 - Twice the results were transposed from one test case to another test reporting page.
- **Failure to follow instructions**
 - Eleven test results were submitted where the instructions had not been strictly followed. In nine of these cases, it was “copying” only one or two additional addresses when the test called for three copies. In some of these cases, the tester reported this was because a third address meeting the test specifications was unavailable.
- **Test Series not executed**
 - The Series 8 tests were never executed (they had been designated as optional) because it was discovered that “REPLY TO:” did not work with an

- o encrypted message that was not also signed. The Challenge did not require a signature.
- o The Series 11 and 12 cases (CAs and Directories) were not executed due to a lack of time and resources. This was a disappointment because they were among the more “challenging” cases.

3.5 Notable Achievements

The key achievement of the Challenge was to construct, test, and demonstrate the architecture described in this document within a 6-month timeframe. Operating with five disparate systems being implemented by three separate organizations spanning nine time zones required substantial coordination. All of this was accomplished on a voluntary basis.

4. Conclusions

4.1 Critical Success Factors

Factor 1: Require documentation that public key actually belongs to intended recipient.

- Certificate policies
- Certificate Practice Statement

Factor 2: Require documentation about safeguarding the infrastructure and encrypted documents

- Relying Party Agreement
- Multi-lateral Agreements

4.2 Lessons Learned

Lesson 1: Keep it simple

- Design an architecture that is flexible enough to allow for different schema
- Require a minimal number of attributes to ensure replication (Challenge 2001 required three: common name, email address, certification)

Lesson 2: Keep costs to a minimum

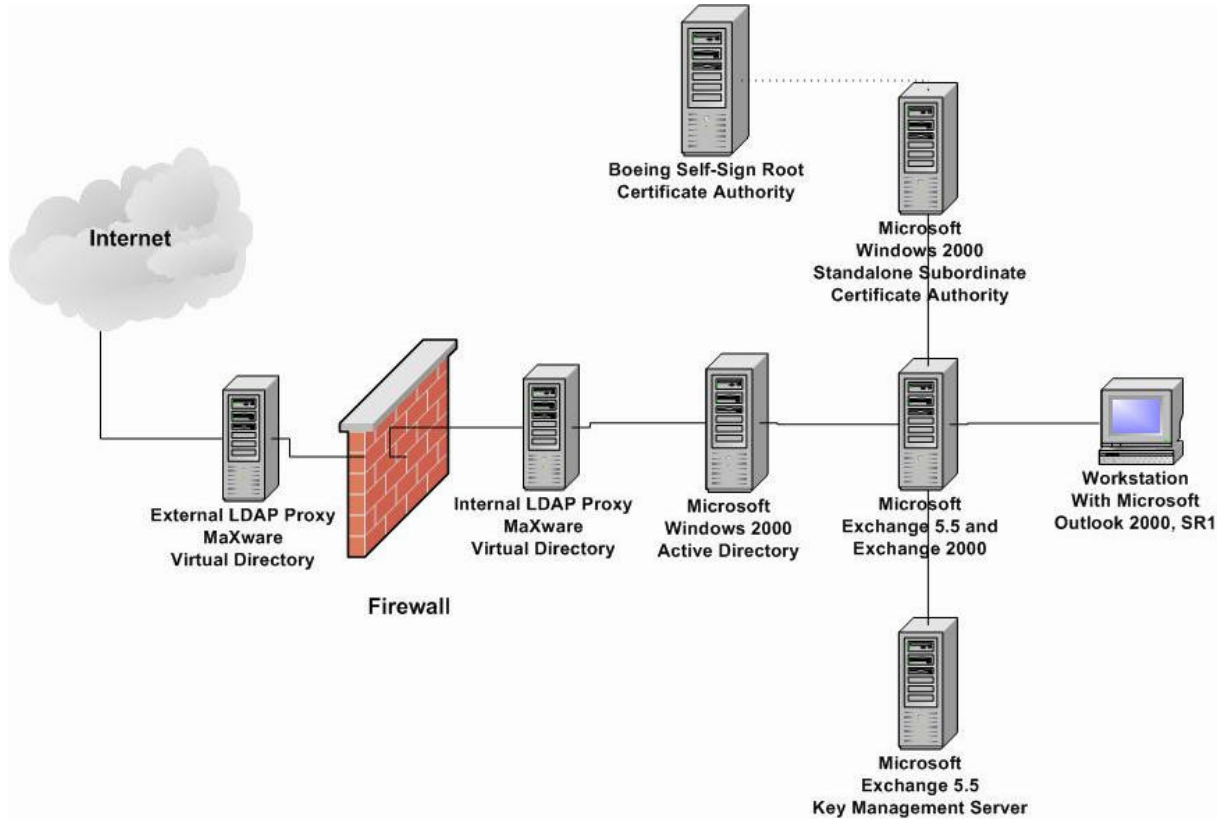
- Use commercial-off-the-shelf (COTS) products

Lesson 3: Use standards-based approach

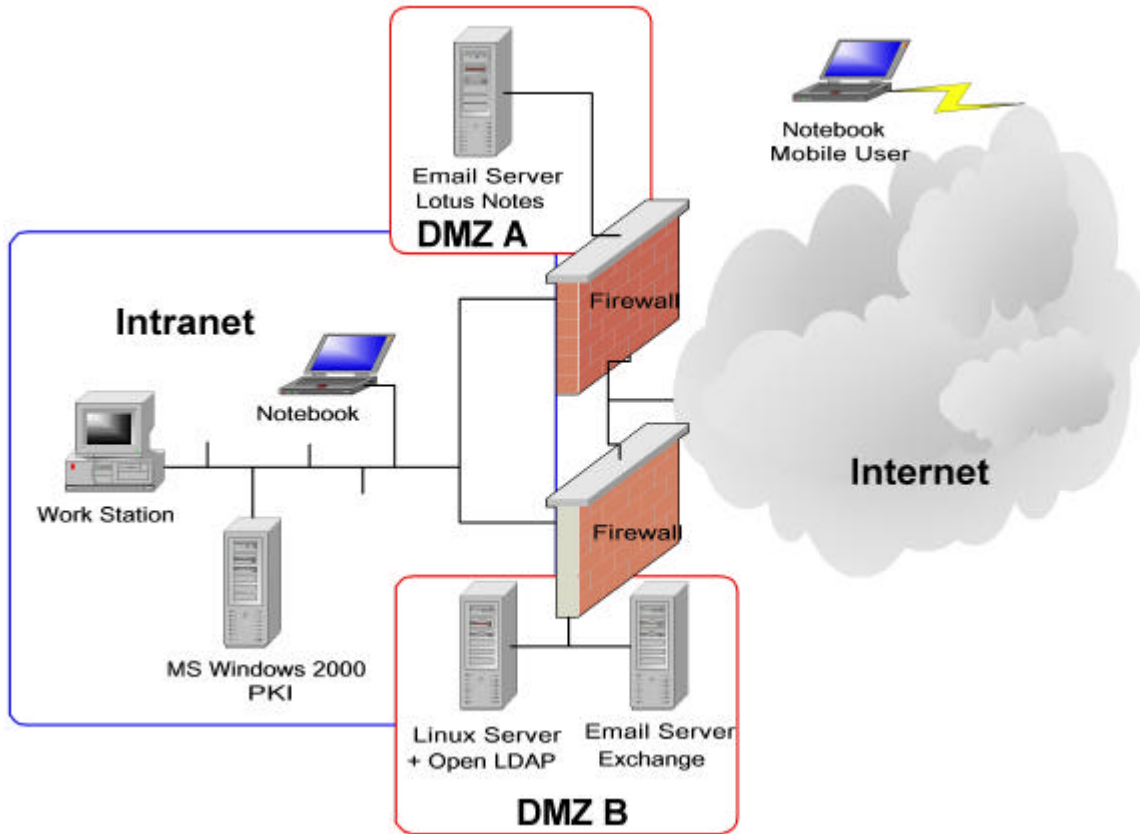
- Leads to excellent vendor and customer support

Because the Challenge Team’s architecture was simple and the cost low, small businesses as well as large corporations can implement it.

Appendix A: Boeing Internal Architecture

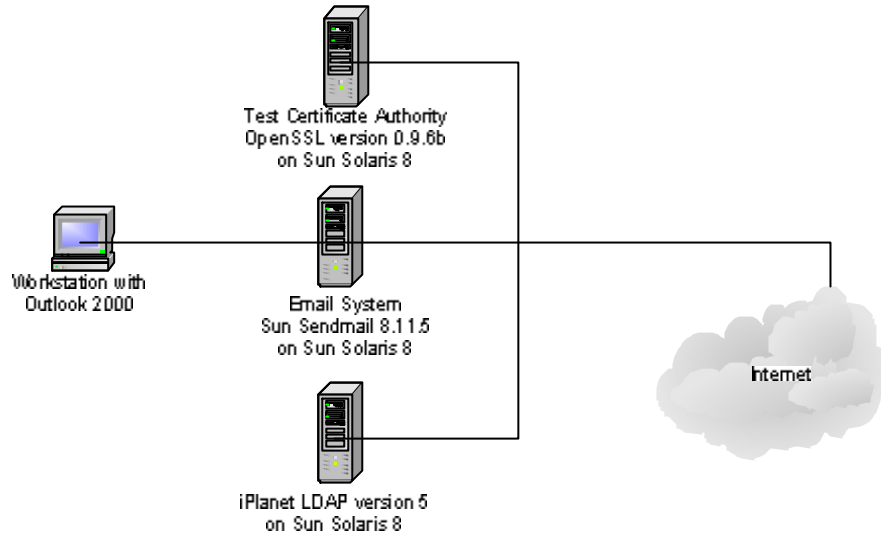


Appendix B: Lynx Internal Architecture



Appendix C: NASA Internal Architecture

SEWP.NASA.GOV Test Environment



Appendix D: smtptestbed.com Internal Architecture

