

Algorithms in PKIX and S/MIME - query

- *To:* <ietf-pkix@xxxxxxx>
 - *Subject:* Algorithms in PKIX and S/MIME - query
 - *From:* "Richard Lampard" <Richard.Lampard@xxxxxxxxxxxxxxxx>
 - *Date:* Wed, 30 May 2001 10:38:41 +0100
 - *Cc:* "Andrew Watson" <Andrew.Watson@xxxxxxxxxxxxxxxx>
 - *List-archive:* <<http://www.imc.org/ietf-pkix/mail-archive/>>
 - *List-id:* <ietf-pkix.imc.org>
 - *List-id:* <ietf-pkix.imc.org>
 - *List-unsubscribe:* <<mailto:ietf-pkix-request@imc.org?body=unsubscribe>>
 - *Sender:* owner-ietf-pkix@xxxxxxxxxxx
-

We recently completed an interoperability trial looking at PKI and S/MIME v3 on
www.cesg.gov.uk/cloudcover/PKIdemonstrator.htm

We are about to embark on a second phase, this time looking at S/MIME v3 en
believe is:

Signature generation: DSA or RSA may be implemented
Signature processing: DSA and RSA must both be supported
Key transport: RSA

However, I also believe that PKIX thinking at the moment is that DSA is sti

This leads to the awkward situation where an implementation, for example, o
DSA. I can imagine other mismatches whereby the keys for one algorithm are

This seems to stem from the fact that thinking on algorithms between PKIX a
play our second phase, and what we should be asking vendors to bring to the
their CAs?

Many thanks

Richard

Richard Lampard
CESG
PO Box 144
Cheltenham
Gloucestershire GL52 5UE

Tel: +441242 221491 x4086

Fax: +441242 709113

This email and any files transmitted with it is intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify

postmaster@xxxxxxxxxxxxxxxxxxxxx

• **Follow-Ups:**

- [Re: Algorithms in PKIX and S/MIME - query](#)

- *From:* Housley, Russ

- Prev by Date: [draft-ietf-pkix-ac509prof -> RFC?](#)
- Next by Date: [Re: cA flag and CRL issuers](#)
- Previous by thread: [Re: cA flag and CRL issuers \(Addendum\)](#)
- Next by thread: [Re: Algorithms in PKIX and S/MIME - query](#)
- Index(es):
 - [Date](#)
 - [Thread](#)



Advanced Security Technologies



Secure Messaging
And
PKI Interoperability Demonstrator
Final Report

Secure Messaging, PKI and Associated Technologies
Within Government.

Issue 1.2

11 May 2001



This document and its content shall only be used for the purpose for which it was issued.
The copyright of this document is reserved and vested in the crown.

©2001 Crown Copyright

FOREWORD

This paper is issued by the Communications-Electronics Security Group (CESG) of Government Communications Headquarters as part of its responsibility to advise HMG on Electronic Information Systems Security (InfoSec).

If you have any questions relating to technical aspects of Interoperability Task please contact the Task Manager. Tel: 01242 221491 ext. 4312. Fax: 01242 709113.
Documentation can be obtained by calling CESG on 01242 221491 ext. 4577.

For information on any other aspects of CESGs work, please contact:

The Marketing Group
Communications-Electronics Security Group
PO Box 144
Cheltenham
Gloucestershire GL52 5UE

Tel: 01242 237323 E-mail: enquiries@cesg.gov.uk

Table of Contents

DEDICATION.....4

EXECUTIVE SUMMARY.....4

1. INTRODUCTION.....5

 1.1 BACKGROUND.....5

 1.2 SCOPE.....5

 1.3 MISSION STATEMENT5

2. PARTICIPANTS AND PRODUCTS6

 2.1 PARTICIPANTS.....6

 2.1 TECHNICAL PRODUCT DESCRIPTIONS.....6

3. SCENARIO12

4. NETWORK ISSUES14

 4.1 DIRECTORIES AND MAIL SERVERS.....14

 4.2 CA KEY STORAGE AND GENERATION14

 4.3 PROTOCOLS14

 4.4 ALGORITHMS.....14

5 TEST PROCESS.....15

 5.1 PLANNING.....15

 5.2 PROCESS.....15

6 PKI & SECURE MESSAGE RESULTS.....16

 6.1 CA INTEROPERABILITY16

 6.2 CLIENT INTEROPERABILITY.....16

 6.3 REVOCATION.....18

7 CONCLUSION.....20

 7.1 PRODUCT INTEROPERABILITY20

 7.2 TEST PROCESS LESSONS LEARNED21

8 FUTURE WORK.....22

APPENDIX A - TEST SUITE STRUCTURE.....23

APPENDIX B - PKI ISSUES27

 B.1 DIRECTORY SCHEMA.....27

 B.2 SUBJECT KEYIDENTIFIER.....27

 B.3 CERTIFICATE ACCEPTANCE27

 B.4 REVOCATION.....27

APPENDIX C - MESSAGING ISSUES30

 C.1 RTF AND PLAIN TEXT30

 C.2 SIGNED (OPAQUE) AND SIGNATURE ONLY (MULTIPART).....30

 C.3 MESSAGE TYPE.....30

 C.4 INCORRECT USE OF ALGORITHM OID30

APPENDIX D - COMPANY CONTACT INFORMATION31

DEDICATION

CESG believes that this is a unique piece of work that significantly reduces the perceived risks associated with the implementation of heterogeneous PKI environments. This work would simply not have been possible without the co-operation of the participating vendors and their willingness to work with one another and invest significant resources in making the trial a success.

The co-operative spirit is an indicator of the increased confidence and maturity of the industry and indicates that the products are now ready for deployment into mainstream applications without representing a significant risk.

CESG would like to extend its thanks to the vendor community for their willing participation and to the Office of the e-Envoy for providing the financial support to make this trial possible.

EXECUTIVE SUMMARY

The PKI & secure messaging interoperability demonstrator aimed to demonstrate the degree of interoperability between products from different PKI and messaging vendors. The scope of the demonstrator covered: certificate request and certificate issue (when operating within a hierarchy) the sending of signed e-mail, certificate revocation and certificate expiry.

To determine the degree of interoperability CESG sponsored a demonstration of commercial PKI and messaging products as applied to a government scenario. Working with commercial PKI and messaging vendors, CESG developed the scenario and test requirements. During the demonstrator CESG provided the basic network infrastructure and overall management, while participating vendors provided the engineers and remaining hardware.

The participating vendors (Baltimore, Compaq, Entegriy, Entrust, Novell, Reflex Magnetics, Shym, Spyrus, SSE, and Xcert (now RSA Security)) demonstrated considerable commitment to the interoperability demonstrator not only providing engineering resources during the demonstrator week, but in the preceding months as well.

The PKI & secure messaging interoperability demonstrator week showed that the vendors have made considerable progress with respect to interoperability. Most of the CA implementations were able to request and accept certificates from the Root CA; the S/MIME v3 client products were able to receive and verify signed e-mail from other vendors' implementations.

The results from the interoperability demonstrated show that the risks of implementing a PKI (for signed e-mail) have been significantly reduced; product interoperability should no longer be viewed as an inhibitor for implementing a PKI.

In line with government policy, the demonstrator used the DSA signing algorithm, SHA-1 hashing algorithm and the S/MIME v3 secure mail protocol.

This document details the findings of the interoperability demonstrator.

1. INTRODUCTION

1.1 Background

- 1.1.1 CESG sponsored, on behalf of the Office of the E-envoy, a PKI and secure messaging interoperability demonstration during February 2001, over a period of 5 days. This work was undertaken because of the belief that the slow uptake in PKI, within HMG, was as a result of the lack of widespread interoperability between different commercial PKI products and PKI enabled applications.
- 1.1.2 The interoperability demonstrator was designed to demonstrate the degree of interoperability that exists between the various certification authority products and PKI enabled secure messaging products. The testing involved the sending of digitally signed messages across a network, where different PKI vendors took on the role of a government department.
- 1.1.3 For the demonstrator CESG provided the accommodation and the central network facilities. The companies who had agreed to participate in the demonstrator provided their own local network and engineers who were responsible for configuring their products to inter-operate with other vendor's products, within the framework of the agreed scenario. Novell provided the Central Directory facilities and Baltimore Technologies provided the Root Certification Authority.

1.2 Scope

- 1.2.1 The scope of the demonstrator was limited to the exchange of signed e-mail between autonomous domains under a common Root. Certificate revocation and certificate expiry were also to be investigated. The highest priority was given to testing the exchange of valid signed e-mail, client revocation and client certificate expiry. The lowest priority was given to testing the effects of CA and Root certificate expiry and revocation.
- 1.2.2 In the event, time constraints meant that only signed e-mail and client revocation were tested.
- 1.2.3 Directory interoperability and confidentiality services were outside the scope of the trial, but where valid results have been obtained, these will be provided for information.

1.3 Mission Statement

- 1.3.1 The aims of the trial were as follows:
 - To provide a catalyst encouraging participating vendors to work together to demonstrate and enhance the degree of interoperability that exists.
 - To demonstrate, to government, the ability of a commercial S/MIME v3 mail client to send and receive signed e-mails, when supported by different commercial PKI products
 - To demonstrate the interoperability that exists between different commercial PKI CA/RA products
 - To demonstrate the interoperability that exists between different commercial mail clients using a basic authentication S/MIME v3 profile.

2. PARTICIPANTS AND PRODUCTS

2.1 Participants

2.1.1 Initially fifteen PKI and S/MIME product vendors agreed to participate in the PKI and Messaging Interoperability Demonstrator. However this number had fallen to nine by the week of the demonstrator, with Novell opting (with the agreement of the other vendors) to provide the central Directory facilities for this phase.

2.3.2 The participants were :

- Baltimore Technologies
- Compaq
- Entegrity Solutions
- Entrust
- Novell
- Reflex Magnetics
- Shym
- Spyrus
- SSE
- XCert (now RSA Security)

2.1.3 The vendors who withdrew from the demonstrator all indicated that they would like to participate in future trials.

2.1 Technical product Descriptions

2.2.1 Overview

The product descriptions contained in the following sections have been supplied by the participating vendors and have been included in good faith. CESG is unable to guarantee that the software used by the vendors in the interoperability week matches that described here - be it the technical detail of each product's functionality and capabilities, or the commercial availability of any specified product version.

2.2.2 *Baltimore Technologies*

CA UniCERT v3.5

UniCERT is a CA system used in PKI systems to provide security for a wide variety of e-commerce and enterprise security systems. It is a modular system using X509v3 digital certificate to provide authentication and non-repudiation for such services as Secure E-mail, Internet shopping, Secure Web Banking etc.

Mail Client Mail Secure v3.1

Baltimore MailSecure is a secure e-mail plugin for the desktop. It provides security and capabilities using the PKI standards. Mail secure also provides the central administration function to enable a security office to manage and control the security settings of groups of users from a central point.

2.2.3 *Compaq*

CA CryptManager v3.1

The Compaq domain consisted the following components:

A Compaq Proliant Server running Microsoft Windows 2000, Microsoft Exchange 2000, the Compaq Exchange(SE) Policy Manager 3.2 Beta and CryptManager 3.1; a second Compaq Proliant Server running Microsoft Windows 2000 Server and the Compaq Exchange(SE) 3.2 Beta Release Authority; and a number of Client systems (Compaq Ipaqs, Compaq Armada Laptops etc) running Windows 2000, Outlook 2000 SR1, the Compaq Exchange(SE) 3.2 Beta Client extension and CryptEasy 3.1.

The Policy Manager (system administrator or security officer) can centrally configure policy that will determine when and how a mail can be sent to a particular destination, this policy is held in a policy matrix which is replicated to each Exchange(SE) Client. The policy Manager can run on any Server in the domain.

When a user creates and sends an e-mail, the Exchange(SE) Client checks the label and the list of addressees against the policy matrix and notifies the user of any discrepancies. Only when all addressees are allowed by the policy is the e-mail sent, encrypting and/or signed by the Exchange(SE) Client as authentication to the Release Authority. This signature contains time and user based parts designed to prevent signatures being reused in a replay style attack.

The release authority acts as an SMTP router with flexible configuration options, it is designed to be extensible to include facilities such as dirty word checking and virus scanning. A e-mail bound out of the domain must pass through the Release Authority and will only be allowed through if the policy requirements have been met and the e-mail carries an electronic signature from the Exchange(SE) Client extension – this signature is release by the Release Authority before the mail is released. Any outbound e-mail arriving at the Release Authority without a signature is rejected and a non-delivery message is generated. Audit facilities can be configured to log all outgoing e-mail, or rejections as required.

The Compaq domain was certified as Sub-CA under the Baltimore Root; Certification, key generation and certificate revocation are provided by CryptManager, while encryption, decryption and digital signatures are provided by CryptEasy.

2.2.4 *Entegrity*

CA Notary v3.1

Entegrity Notary v3.1 is a CA product that enables business and end users to create, sign, distribute, verify, use and revoke digital certificates. It supports cross-certification between domains, encryption including Diffie-Hellman, RSA, DSA, and is policy driven for easy administration.

Mail Client Assure Mail v3.1 (Beta)

Entegrity Assure Mail supports S/MIME v3, including security labelling and provides policy driven protection of e-mail to minimise the impact on the user. It provides a plug in for Microsoft Outlook and support all common SMTP clients such as Microsoft Outlook and Eudora.

2.2.5 *Entrust*

Public Key Infrastructure

Entrust Technologies provided Entrust/PKI™ Release 5.1 that has been commercially available since November 2000. Entrust/PKI consists of two main components, Entrust/Authority™; the server based Certification Authority, and Entrust/RA™, the distributed registration and administration client software. Entrust/PKI™ can issue a range of certificates, for example for desktop applications, Internet transactions, electronic commerce, developer applications, wireless devices and access control devices, either as fully automatically managed certificates or unmanaged certificates.

Entrust/Entelligence™ is an optional part of Entrust/PKI™ which resides on the desktop and is seamlessly integrated into the Microsoft® Windows 95/98 Windows NT 4.0 and Windows 2000 desktop operating system and underpins the Entrust Desktop Suite of products. The role of Entrust/Entelligence™ is to interface with the server components and provide such services as dynamic policy control, revocation status checking, automatic key and certificate lifecycle management, user roaming and controlled access to the cryptographic routines and user's credentials. Included in Entrust/Entelligence™ are APIs that allow applications to become enabled to the PKI and benefit from a single login to the managed security infrastructure, evidenced by the extensive range of Entrust Ready partner products. Entrust Desk Top Solution V6.0 Beta

The S/MIME v3 email solution is provided by a combination of Entrust/Entelligence Release 6.0 beta (due for release Q201) and Microsoft Outlook 2000 with SP1. The additional feature provided by Release 6.0 of relevance to the demonstrator is the ability to synchronise the keys and certificates managed by Entelligence with the Microsoft CAPI key store where they can be used by CAPI-enabled applications; in this case Outlook 2000.

2.2.6 *Novell*

Novell NDS eDirectory8.5

Novell NDS eDirectory supports PKI interoperability by providing a central repository for storing the various PKI vendors certificates and certificate revocation lists (CRLs). The Novell NDS eDirectory allows each vendor to publish its certificates and CRLS within this common directory service.

Users of each of the PKI services can query the directory to retrieve certificates created by any of the PKI services, and check to see if these certificates have expired or been revoked.

Support for Lightweight Directory Access Protocol (LDAP) ensures that this approach works in an Internet environment between commercial organisations wishing to exchange confidential information across a public network.

2.2.7 *Reflex Magnetics*

Reflex MailSafe Enterprise version 1.1 consists of the following components:

- Reflex MailSafe Certificate Authority
- Reflex MailSafe Central Configuration Server
- Reflex MailSafe Client

Reflex MailSafe Certificate Authority

Reflex MailSafe Certificate Authority allows an organisation to manage the issue, renewal, and revocation of digital certificates through the provision of customisable services for the issue and management of X509 digital certificate. The Certificate Authority combined with Microsoft Exchange Server LDAP directory provides a way of enabling secure e-mail facility for all users within an organisation.

Reflex MailSafe Configuration Server

The Configuration Server administrator can centrally specify various Mail Safe Client settings; preferred cryptographic algorithms, list directories where to search for certificates and revocation lists, list trusted certificates etc. Configuration settings are distributed to client machines according to a schedule in a digitally signed form, thus enforcing configuration data integrity.

MailSafe Client version 2.1

Reflex MailSafe Client provides an S/MIME v3 compatible solution to e-mail security by integrating to Microsoft Exchange, Outlook 9x and Outlook 2000. Reflex MailSafe Client does not limit Outlook features like Rich Text, HTML, distribution lists are available for secure messaging and supports secure receipts and security labels.

2.2.8 *Shym*

MailShym for Outlook 2000 (SP1)

Message Format: S/MIME v3, excepting all generated messages are generated as multipart only.

Certificate Support: DSA, RSA (all formats) via SIL/SPI (see below)

Desktop Repository of Certificates: CAPI v2 (128) bit, BSAFE, Entrust Desktop (V4,v5), SmartCards via CSP/CAPI.

Shym Integration Layer

Provides transport and protocol support between Application Shym, LDAP Directories, Validation Services, Logging, and PKI vendor specific implementation features.

Directory Access: LDAPv3 and LDAPv2, with SSLv3 and SSLv2, or open transport as required.

Shym Provider Interface (SPI)

The SPI provides the low level access for certificate support, specific to each PKI vendors implementation. Generic X509, Baltimore, Microsoft, iPlanet, version, Xcert/RSA certificates are processed in a similar fashion, excepting some checking. Two SPI versions are available for each certificate vendor, CAPI (mainly non-session based applications) and BSAFE (for session based applications).

Entrust Desktop (with Entrust certificates) is also supported (v4 and v5), taking into account the storage of keys in the EPF file. For S/MIME processing, additionally, the target mails users x509 certificate is automatically transferred into the local users Entrust Local Address.

Book before the S/MIME operation proceeds. The Entrust SPI may be used for both session, and non-session based Application Shyms.

2.2.9 *Spyrus*

Spyrus PKI Production Build 17

Consists of the following software applications

- Spyrus PKI Policy Approval Authority (PAA)
- Spyrus PKI Policy Creation Authority (PCA)
- Spyrus PKI Organisational Certification Authority (OCA)
- Spyrus PKI Organisational Registration Authority (ORA)
- Spyrus Web Registration Software
- Spyrus LYNKS privacy cards
- Spyrus RD300 Readers

The Spyrus PKI is a security architecture designed for ITSEC E3 and Common Criteria EAL4 Evaluation. The Spyrus LYNKS privacy card provides cryptographic operations for the PAA, PCA, OCA and ORA. The Spyrus LYNKS card is a tamper evident device that supports: SHA-1, MD5, RSA (512, 768, 1024, 2048 bits), DSA (1024 bits), Diffie-Hellman, KEA, DES Triple DES, Skipjack and a FIPS 140-1 approved hardware random number generator. The PAA and PCA are off line components that are used to create the root and subordinate keys on the LYNKS cards. The PCA defines the certificate policies that are enforced by the OCA. The OCA is designed for 'lights out' automated operation and processes certificate requests from a registration administrator using the ORA application software. Communications between the OCA and ORA are encrypted and each certificate request is logged in the OCA database. The ORA incorporates a Programmable Policy Module (PPM) that enables an organisation to define and implement their own policies and security levels. The Spyrus Web Registration is a web server based application that enables an end-user to post certificate request and download signed certificates from an LDAP directory.

Mail Client Microsoft Outlook 2000

No third-part plug-in for revocation was deployed for the Demonstrator.

In the demonstrator, Microsoft Outlook 2000 was used in conjunction with Spyrus USB tokens, Spyrus Rosetta smart cards and Spyrus PAR2 (Personal Access Reader).

2.2.10 SSE

Mail Client SSE Trusted MIME v2.25

TrustedMIME is a client-side secure e-mail solution based on the S/MIME protocol. TrustedMIME plugs into Microsoft (Outlook 97/98/2000, Exchange, Messaging) and Lotus Notes (4.5, 4.6, 5.0) e-mail clients, providing strong (128-bit) encryption and (up to 2048-bit) digital signatures to secure the e-mail client.

TrustedMIME/Corporate is an add-on tool to the core solution, which enables an organisation to customise TrustedMIME to implement its security policy. Using TrustedMIME/Corporate, an organisation can define and enforce an enterprise-wide policy for secure e-mail. This enables administrators to pre-configure encryption and digital signature policies from a central point.

TrustedMIME can work with the organisations chosen Public Key Infrastructure (PKI). For existing PKIs, TrustedMIME can work with external, Commercial Certification Authorities (CAs) and also provides a range of options for working with internal, local CAs. In the absence of an existing PKI, TrustedMIME users can generate their own self-signed Public Key Certificates. TrustedMIME supports the latest standards including S/MIME version 3, OCSP and LDAP version 3. In addition, the TrustedMIME SDK allows partners and resellers to integrate core product functionality into an organisation's existing applications.

2.2.11 XCert

CA Sentry v4.5.1

The vendor did not supply a description of the products used in the Demonstrator.

3. SCENARIO

- 3.1 The UK Government has a requirement for each government department to communicate, by e-mail, with other departments and external organisations. The E-Governments Interoperability Framework eGIF of September 2000 (<http://www.govtalk.gov.uk/egif/interop>) specifies the use of S/MIME v3 over SMTP. It is anticipated that each government department will implement its own PKI, using different commercial PKI and messaging products, which will operate within a hierarchy under the HMG Root Authority CA. The communication between each department, and to external organisations, requires the use of digital signatures and certificates as a mechanism for providing message authentication, integrity and non-repudiation of origin.
- 3.2 The test scenario was designed to model this state of affairs and is illustrated in Figure 1. Each PKI vendor provided a domain (analogous to a government department) consisting of a certification authority and one or more secure messaging clients. Some domains operated a mixed client environment. All CAs were certified under a common Root authority.
- 3.3 Directory services were provided centrally by a product that all vendors agreed to use prior to the trial. Directory interoperability testing was not within the scope of the trial.
- 3.4 The aim was to demonstrate the PKI Interoperability of diverse PKI solutions using S/MIME messaging as a vehicle to prove this.

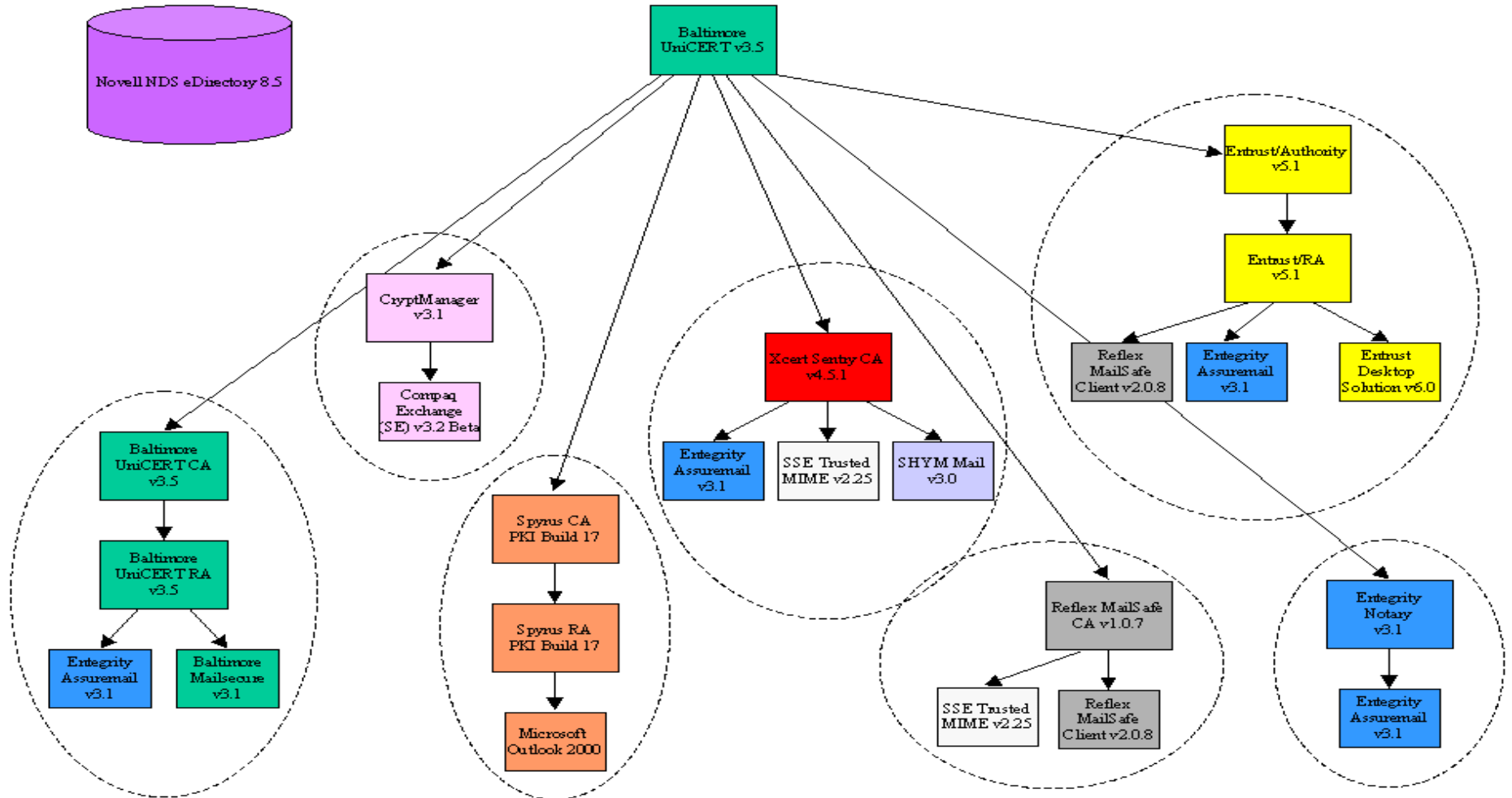


Figure 1. Interoperability Demonstration Network

4. NETWORK ISSUES

4.1 Directories and Mail Servers

4.1.1 The participating vendors agreed to use the Novell NDS eDirectory 8.5 as the Central Directory (and had access to this directory for testing before hand). Novell provided support for the directory during the demonstrator week as a means of mitigating the risk of any directory issues.

4.2 CA Key Storage and Generation

4.2.1 Vendors generated their own public and private keys, as well as their own DSA parameters which were then certified under a central root CA.

4.3 Protocols

4.3.1 There are several stages within a certificate and e-mail life cycle each with its own protocols. These were agreed as a minimum level of interoperability prior to the demonstration as a minimum level of interoperability, as identified in the Table 1.

Certificate/Messaging Stage	Standards	Protocols
Certificate Request for CA to CA	PKCS#7 PKCS#10 (no attributes)	File transfer via shared directory
Certificate Generation	Min. Requirements of RFC2459	
Certificate Verification	Min. Requirements of RFC2459	
Certificate Revocation	Min. Requirements of RFC2459	
Messaging	RFC 2630, RFC 2633	S/MIME v3 (using CMSG supplied profile)
Network Transfer		TCP/IP
Directory Access		LDAP v3

Table 1: Certificate and Messaging Standards and Protocols

4.4 Algorithms

4.4.1 For the purposes of the interoperability demonstration, it was proposed to test only the implementation of digital signatures using 1024 bit DSA, with SHA-1, as this was the minimum requirement of RFC 2630 at the time of the trial and the HMG preferred algorithm for digital signatures.

5 TEST PROCESS

5.1 Planning

- 5.1.1 The tests, which were to be carried out, were initially planned using a test suite structure as shown in Appendix A. The use of the chart enabled CESSG to identify all the tests required to validate the functionality of each product with respect to Certificate Request and Issue, Data Integrity, Signing Messages, Certificate Revocation and Certificate Expiry.
- 5.1.2 Consultation with the vendors indicated that some of the tests (for example CA Certificate Revocation), for some products, were destructive and would require a system rebuild (for example, revoking a CA certificate may require the CA software to be re-installed and configured). Such tests were, therefore deferred until the end of the testing process, and were afforded a lower priority

5.2 Process

- 5.2.1 The test process, employed by CESSG, was to allow a period of informal testing until the majority of the participants were content that they had achieved interoperability. At that point, a halt was called to the informal testing, and a controlled test was performed covering each vendor in turn.
- 5.2.2 Vendors whose products were unsuccessful, or who were not ready to perform the tests were given an opportunity to re-perform the tests at a later time. Between each formal test, time was given to allow the participating vendors an opportunity for testing between other products.

6 PKI & SECURE MESSAGE RESULTS

- 6.01 These results detail the findings of the PKI & Secure Messaging Demonstrator held at CESG in February 2001. The results have been interpreted from the state of play at the end of the week when a lot of the initial configuration problems had been resolved.
- 6.02 When reading the results it should be understood that the results are based on a product's ability to read a message (and validate a signature) of a message sent from another client product. The inability of a product to achieve this does not mean that the fault is with the recipient (unless indicated otherwise). It was out of the scope of this project to decode the messages sent and attribute fault to any one vendor product. It should also be noted that some of the products are still beta as indicated in section 2.

6.1 CA Interoperability

- 6.1.1 All the vendor CA implementations were able to request and accept sub-CA certificates from the UniCERT Root CA, with the exception of Entegrity and Spyrus.
- 6.1.2 Spyrus required an additional utility programme to achieve this. Representatives, participating in the demonstrator indicated that this utility would be incorporated into a subsequent product release.
- 6.1.3 The Entegrity Notary CA could not accept the sub-CA certificate generated by UniCERT as the UniCERT sub-CA certificate and root certificate contained an extension that was not part of the agreed certificate format for the interoperability demonstrator - as defined in section 4.4.1 of this report. Entegrity's engineering team modified their PKIBench Tool to support this optional feature and were able to successfully accept the sub-CA certificate following the modification. Entegrity Notary will include support for this optional feature in its next release.

6.2 Client Interoperability

- 6.2.1 Most of the client products were able to receive and validate signed (opaque) and signature only (multipart) messages sent from all other vendor implementations. RFC 2633 does not mandate the use of either opaque or multipart for sending or receiving messages leaving the options open for varying implementations. It is therefore possible for two different implementations to meet the requirements of RFC2633 and not be able to receive and validate messages from another implementation.
- 6.2.2 *Baltimore Mail Secure*
- Mail Secure was able to receive and validate messages both opaque and multipart sent from all other vendors. However, there were issues with messages containing attachments sent from AssureMail. Specifically, in some cases the attachment content appeared garbled or the attachment title was lost, but the signature appeared to be verified.
- 6.2.3 *Compaq Exchange(SE)*
- The *Exchange(SE)* product will not send multipart messages, however it is capable of receiving, and validating both opaque and multipart messages. *Exchange(SE)* was able to receive and validate messages from all other client implementations. The only exception was that *Exchange(SE)* could not receive opaque messages with attachments from the SSE Trusted MIME client in the Reflex Magnetics domain, however it could receive from the SSE Trusted MIME client in the Xcert domain.

6.2.4 Entegriy *AssureMail*

AssureMail was able to receive and validate messages sent from most other client implementations, with the following exceptions:

- from the Spyrus domain using the Microsoft Outlook client.
- from the SSE Trusted MIME in the XCert domain.
- from Compaq Exchange(SE) for the AssureMail client in the Entrust domain, although no problems were experienced with AssureMail clients in other domains when receiving from Compaq.

Entegriy detected that both the Spyrus domain, using the Microsoft Outlook client, and Trusted MIME implementations were using an incorrect OID to represent the DSA algorithm in their signed messages. No other vendor detected this.

Entegriy also detected that MailSecure was using an inappropriate (MISSI) OID, other products did not.

6.2.5 *Entrust Desktop Solution*

The Entrust Desktop implementation was able to receive and verify messages from all other client implementations.

6.2.6 *Reflex MailSafe*

The MailSafe implementation was able to receive and verify messages from all other client implementations.

6.2.7 *SSE Trusted MIME*

Trusted MIME was able to receive and verify messages from all other client implementations. With messages received from Spyrus domain, there was an additional attachment received which could not be opened.

Trusted MIME requires the user to explicitly accept a certificate, which it then places in an address book. This makes it difficult to verify that the product is correctly validating the certificate path.

6.2.8 *Shym Mail*

The Shym Mail client could not send or receive opaque messages but it was able to receive and validate multipart messages from Mail Secure, Trusted MIME clients in both the Reflex Magnetics and XCert domains, and the Spyrus, domain using the Microsoft Outlook client. It could not successfully receive and validate messages from other clients.

Shym Mail requires the user to explicitly accept a certificate, which it then places in an address book. This makes it difficult to verify that the product is correctly validating the certificate path.

6.2.9 Spyrus Domain using the Microsoft Outlook client

The Spyrus domain, using the Microsoft Outlook Client, could receive opaque messages all other client implementations except for AssureMail in the Entegriy domain.

The Spyrus domain, using the Microsoft Outlook client, could validate multipart messages without attachments from the following implementations

- MailSecure
- All clients in the Entrust domain
- All clients in the Reflex Magnetics domain

It could not validate multipart messages with attachments from the following implementations

- AssureMail in the Baltimore, Entegrity and Xcert domains
- Trusted MIME or Shym in the Xcert domain

The Spyrus domain, using the Microsoft Outlook client, could validate multipart messages with attachments from all clients in the Entrust domain. It could not validate multipart messages with attachments from the following implementations

- AssureMail in the Baltimore, Entegrity and Xcert domains
- Trusted MIME or Shym in the Xcert domain

Other cases were not tested.

6.3 Revocation

6.3.1 Mail Secure

Mail Secure was able to check the revocation status of clients in both its own and other domains, with the exception of the Entegrity domain, for which Mail Secure was unable to locate the CRL.

6.3.2 Exchange(SE)

Exchange(SE) was able to verify the revocation status of all clients in both its own and other domains.

6.3.3 AssureMail

AssureMail was able to identify the revocation status of clients as follows:

- AssureMail in the Baltimore domain was able to correctly determine that the certificates of AssureMail clients in other domains had been revoked. However, while AssureMail did not detect that certificates had been revoked it did detect that a certificate was not valid for the Compaq and Reflex Magnetics domains. Time constraints meant that the SSE Trusted MIME and Shym Mail clients in the XCert domain were not tested.
- AssureMail in the Entegrity domain was able to correctly determine that the certificates of the AssureMail client in the XCert domain had been revoked. However, while AssureMail did not detect that certificates had been revoked it did detect that a certificate was not valid for the Compaq and Reflex Magnetics domains. Time constraints meant that the SSE Trusted MIME and Shym Mail clients in the XCert domain were not tested.
- AssureMail in the Entrust domain was able to correctly determine that the certificates of the Shym client in the XCert domain had been revoked. However, while AssureMail did not detect that certificates had been revoked it did detect that a certificate was not valid for the Compaq and Reflex Magnetics domains. Time constraints meant that the SSE Trusted MIME and AssureMail clients in the XCert domain were not tested.
- AssureMail in the XCert domain was able to correctly determine that the certificates of Mail Secure, Compaq Exchange(SE), Entrust Desktop Solution, Reflex MailSafe in both the Entrust and Reflex domains, SSE Trusted MIME in the Reflex domain and Shym Mail had been revoked. Time constraints meant that the AssureMail client in the Baltimore domain was not tested.

Entegrity AssureMail checks the revocation status of a message at the time it is signed if a signing time attribute is detected. Both the Compaq and Reflex Magnetics

domains supplied signing time attributes and AssureMail flagged their certificates as invalid but not revoked as a suitable historic CRL could not be located to check the validity of the certificates. Entegriy are to change the way that this historical revocation checking is performed in later releases of AssureMail as there is a potential for interoperability problems and confusion by other vendors.

When a signing time attribute is not present Entegriy AssureMail checks for revocation status in strict accordance with the rules specified in RFC2459, and caches valid CRLs for efficiency purposes until they expire. The revocation test used in the interoperability week assumed the mail clients did not cache valid CRLs. As AssureMail already had valid in-date CRLs for the other domains in its cache, it followed the rules of RFC2459 and used those CRLs when validating the test messages - they were therefore correctly reported as not revoked. This is the correct behaviour as laid down by RFC2459. The revocation test should have been performed using a regularly periodic CRL not using an unscheduled forced CRL. RFC2459 is quite clear that a CA cannot assume that a forced CRL will be used and that revocation will only be enforced following the issuance of the next expected periodic CRL.

6.3.4 *Entrust Desktop Solution*

Entrust Desktop Solution was able to verify the revocation status of all clients in both in its own and other domains.

6.3.5 *Reflex Magnetics Mail Safe*

Mail Safe was able to verify the revocation status of all clients in all both in its own and other domains.

6.3.6 *SSE Trusted MIME*

Trusted MIME was able to verify the revocation status of certificates as follows:

- Trusted MIME in the Reflex Magnetics domain was able to detect that certificates from the Spyrus domain, using the Microsoft Outlook client, had been revoked. Time constraints meant that tests were not performed against clients in the XCert domain.
- Trusted MIME in the XCert domain was able to detect that certificates from Entegriy AssureMail in the Entegriy domain, both Reflex Magnetics MailSafe clients, SSE Trusted MIME in the Reflex Magnetics domain, and the Spyrus domain, using the Microsoft Outlook client, had been revoked. Time constraints meant that tests were not performed against clients in the XCert domain.

6.3.7 *Microsoft Outlook 2000*

Due to a revocation plug in not being available at the time of testing, revocation tests with the Microsoft Outlook 2000 client were invalid.

6.3.8 *Shym Mail*

Revocation tests were not performed with the Shym Mail client as engineering support was not available during these tests.

7 CONCLUSION

7.1 Product Interoperability

- 7.1.1 Although interoperability trials have been carried out before, this trial was probably one of the most complex undertaken, and most if not all the products tested had not been exposed to such a heterogeneous environment. It was discovered that interoperability can be severely affected issues such as the S/MIME wrapping mechanism employed and by non-security relevant issues such as the message format (plain text versus RTF). There is also still a significant amount of work to be undertaken by the vendors to resolve the problems associated with revocation. Of the vendors participating in the interoperability demonstrator, approximately 50% were able to successfully demonstrate that they could correctly validate the revocation status of signed message from all other participating vendor implementations. The remaining products had varying degrees of success, from an inability to check the revocation status of messages sent from the majority of domains, to verifying the correct revocation status of some messages and indicating that there was a problem with the certificate with other messages
- 7.1.2 The PKI & Interoperability demonstrator week showed that the vendors have made considerable progress with respect to interoperability. Most of the CA implementations were able to request and accept certificates from the Root CA; the S/MIME v3 client products were able to receive and verify signed e-mail from other vendor's implementations. In particular, the aims described in the mission statement in Section 1.3 were all achieved. It is very apparent that vendors have invested a considerable amount of time and effort on resolving interoperability issues over the past year.
- 7.1.3 The aims of the trial were as follows:
- To provide a catalyst encouraging participating vendors to work together to demonstrate and enhance the degree of interoperability that exists. This was very successfully achieved.
 - To demonstrate, to government, the ability of a commercial S/MIME v3 mail client to send and receive signed e-mails, when supported by different commercial PKI products. This was partially successful. The ability of most PKIs to issue certificates to a range of products was successfully demonstrated, but the inability of some products to validate the revocation status is a concern. However, it should be recognised that some of the implementations were used during the demonstrator were beta code.
 - To demonstrate the interoperability that exists between different commercial PKI CA/RA products. This was successfully achieved.
 - To demonstrate the interoperability that exists between different commercial mail clients using a basic authentication S/MIME v3 profile. This was largely successful. Most products could process messages from all other client implementations in some form. However only three could do so with no (or minor) issues, all of which could also handle all revocation information. Some of the issues can be avoided by sending acceptable formats (opaque v multipart; text v RTF; etc) but this puts constraints on the sender.
- 7.1.4 The majority of problems encountered during the week were, for the most part, caused by configuration issues. Those vendors whose products did experience problems have indicated that as a result of this trial these problems will be resolved in their next product releases.

7.1.5 The results from the interoperability tests demonstrate that concerns of interoperability should no longer be viewed as an inhibitor for implementing a PKI. Interoperability problems will be encountered, but with willing participation from the vendors, they are resolvable. The level of interoperability of S/MIME v3 mail clients is less well defined but companies are committed to resolving the issues shown up in the tests.

7.2 Test process lessons learned

7.2.1 The large and complex test plan illustrated in Appendix B proved to be unworkable in practice, and is more appropriate to an environment where testing can be largely automated (e.g. conformance testing). The number of vendors participating in the trial also made it very difficult to manage the testing process. A better approach seems to be to allow participants a period of informal testing, followed by a breakpoint, in which a set of tests (e.g. sending a signed message from one client to all other clients and verifying its correct receipt) is carried out systematically. This testing is laborious and time consuming, but seems to be the only way in which meaningful results can be derived.

7.2.2 The degree of conformance to the profiles defined before the trial (in particular the S/MIME profile supplied by CESG) was highly variable. The lesson here seems to be that more effort should be put into defining and ensuring compliance with profiles before a trial, and less effort should be put into the development of large and complex test suites.

7.2.3 There is clearly a greater need to be more pro-active in the direction of pre-trial testing. This was left to the vendors to undertake, but the result was that such testing was carried out behind closed doors between small groups of cooperating vendors. As a result, during the trial week, some vendors were considerably better prepared than others. Certainly the trial week constituted the most complex operating environment that many of the products had encountered up to that point.

7.2.4 The lack of a reference implementation against which to test the products made it difficult to establish the source of many interoperability problems. In addition, where client products successfully received and validated signed messages that had known faults (e.g. incorrect OIDs), it was not clear whether the recipient was adopting a relaxed validation regime, or whether certain checks were not being carried out at all. A reference implementation would help to resolve this.

7.2.5 Minor issues also complicated testing that only came to light during the trial.

- a. Although domain names and network addresses were defined in advance, client names and email addresses were not. This often made it difficult to resolve which messages had been received from which client without the constant need to check with the sender.
- b. Much of the equipment used by the vendors for testing was demonstration kit used for marketing events. This makes it difficult for them to tie the equipment up for long periods of pre-trial testing. The lesson here is for vendors, that they must be prepared to commit resources to testing that will not be removed at short notice.
- c. The revocation tests involved the sending of a message, queuing this message at the mail server while the relevant certificate was revoked, then allowing the message to reach the recipient. However, forcing a CRL to be published in this

way caused problems, as the previous CRL would still be valid. This caused confusion over the interpretation of the results.

8 FUTURE WORK

- 8.1 It is planned to undertake a second phase of interoperability testing. This work will concentrate on different aspects of interoperability attainable between commercial-off-the-shelf PKI and messaging products. The aspects to be tested are still to be scoped out, but will include the exchange of encrypted messages.
- 8.2 Accomplishment of the objectives is largely dependent upon the willing participation of the vendors, who must be willing to have the findings published in a report on completion of this phase. The results will also be forwarded to the PKI Forum.
- 8.3 Future work will be taken forward as part of a collaborative programme with the PKI Forum and the EEMA PKI Challenge.

APPENDIX A
TEST SUITE STRUCTURE

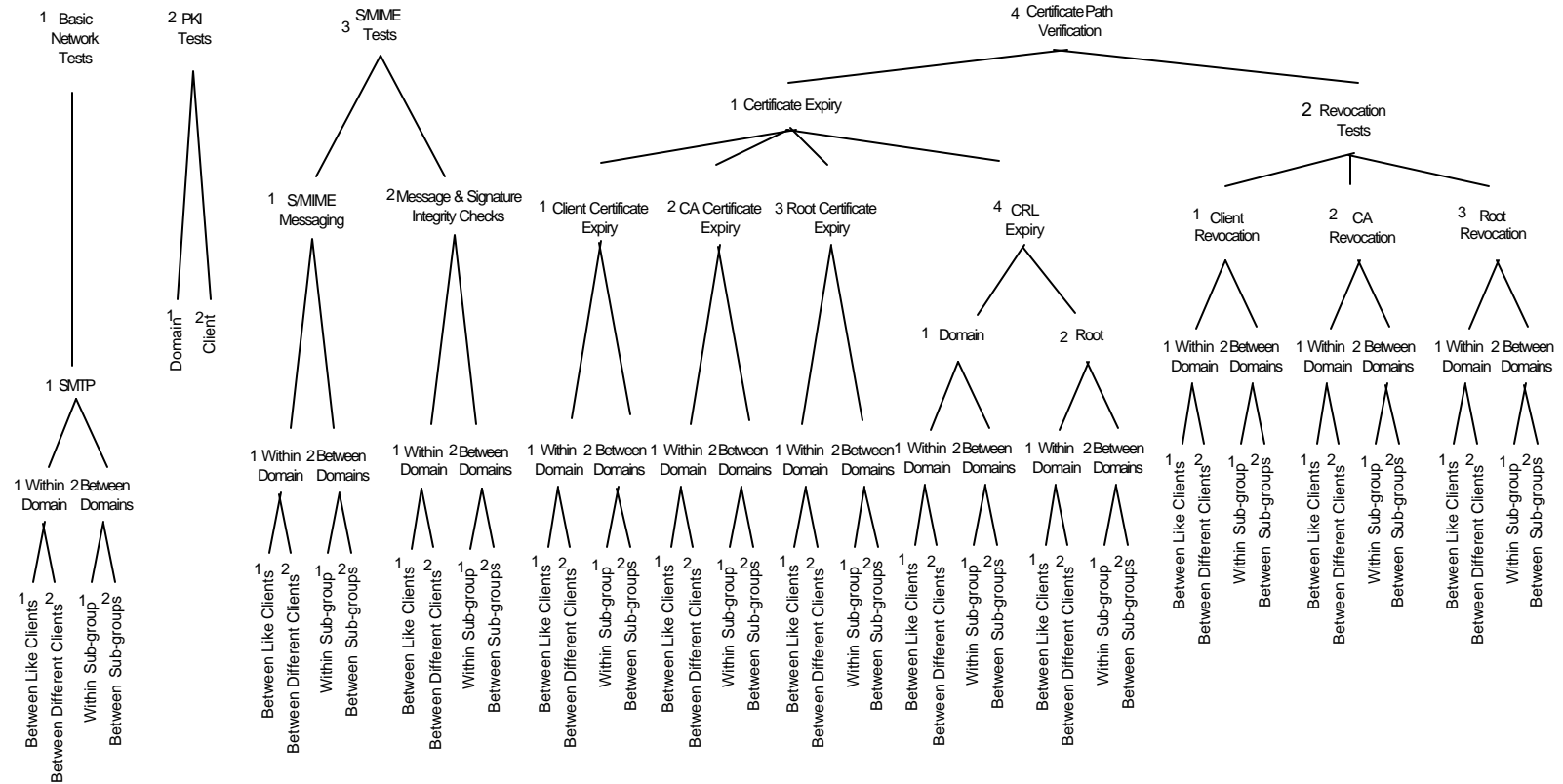


Fig.2 PKI & Messaging Tests

APPENDIX B
PKI ISSUES

B PKI ISSUES

B.0.1 The process of certifying each domain CA by the Root Authority proceeded with few problems. This shows that it is feasible to operate a mixed hierarchy of CA products. However, a number of PKI related issues did arise which are described below.

B.1 Directory schema

B.1.1 The directory structure schemas employed by the participants for the storage of certificates and revocation information differed between the various vendors. This was the greatest cause of PKI interoperability problems.

B.1.2 Some client products are flexible enough to be able to cope with different directory schemas, and can recurse through the DIT until the required information is found. Other client products proved to be less flexible, and would not be able to validate the certificate, if certificates or revocation information were not found in the expected location for their specific directory schema.

B.2 subjectKeyIdentifier

B.2.1 A problem with key identifiers was noted. The certificate request protocol used, PKCS#10, does not specify how key identifiers should be agreed between requestor and issuer. A problem arose in that the certificate requestor expected the key identifier to be calculated in a particular manner, while the issuing authority calculated the key identifier using a different method before returning the certificate. This meant that mismatches arose in the certificate chain between the AuthorityKeyIdentifier in one certificate, and the SubjectKeyIdentifier in the issuing authority's certificate.

B.2.2 RFC2459 suggests two different methods of calculating the key identifier, and further, does not mandate any particular method to be used.

B.3 Certificate acceptance

B.3.1 Some of the CA and client products require the user to explicitly accept a certificate before it can be stored in the address book. Such a feature makes it difficult to ascertain whether the client product is genuinely checking the certification path.

B.4 Revocation

B.4.1 The revocation tests were carried out by sending a message from each client within a domain. Each message was held at the central mail server temporarily preventing delivery to recipient systems. While held at the mail server each of the client certificates was revoked, and the relevant CRL was updated and published to the directory before the messages were released from the central mail server. The updated CRL was issued before the normal scheduled CRL issue.

B.4.2 Approximately half of the client products were able to successfully validate the revocation status of the certificates. Some products indicated that the certificate had not been revoked but did indicate that the certificate was not valid. Other products showed an internal error. The cause of the problems was not clear, although they may be partially related to the inability of some client products to retrieve revocation information from the directory using a schema not supported by that product.

B.4.3 A problem encountered was that at least one client product checked to see if the message was valid at the time of signing rather than at the time of validation - for historical archiving support purposes. This potentially has the problem that if there is a compromise, a message could be forged to look as if it was valid at the time of signing. However, the vendor has indicated that the way that historical revocation

checking is performed will be changed in later releases due to its potential for interoperability problems and confusion by other vendors.

- B.4.4 The revocation test used in the interoperability week used forced CRLs. This test, although beyond the rules described in RFC2459 and outside the scope of what was expected by the vendors, was useful in that it confirmed the warning in RFC2459 that those running a CA can not guarantee that revocation information in a forced CRL will reach the end-user client applications. This enforces the message that if immediate revocation status promulgation is required then either online revocation checking should be performed - using say OCSP - or an extremely low CRL period should be used.

APPENDIX C
MESSAGING ISSUES

C. MESSAGING ISSUES

C.0.1 A number of interoperability issues encountered during the trial centred on messaging. They are described below. Note that in many cases it could not be resolved whether the sender or receiving client was the cause of the problem.

C.1 RTF and plain text

C.1.1 Some vendors had difficulty receiving and processing messages in rich text format (RTF), and could only display messages in plain text format.

C.1.2 Other vendors while capable of receiving RTF would only allow plain text messages to be sent.

C.1.3 It was not possible to determine during the trial the cause of this difficulty.

C.2 Signed (opaque) and signature only (multipart)

C.2.1 Support for opaque and multipart format messages differed between products. For example, the different mail clients could either:

- a. send and receive messages in either opaque or multipart format;
- b. receive both opaque and multipart messages but only send in the opaque format;
- c. only send and receive in multipart format.

C.3 Message type

C.3.1 Within the Message Application Programme Interface (MAPI) properties which are set to indicate that an attachment is called smime.p7m. These properties are short filename, long filename, filename and display name.

C.3.2 One of the participating vendors used two of these properties while a recipient checked different properties, so was unable to determine whether the message type was S/MIME.

C.3.3 The problem was resolved by both vendors modifying their code, one to set all the properties when sending, the other to check all the properties when receiving.

C.4 Incorrect use of algorithm OID

C.4.1 One of the participating vendor's products used an old (MISSI) OID for DSA. Some products detected this and would not accept the message as it contained an invalid OID. Other products accepted the message without any warnings.

C.4.2 In another instance, a client product used the DSA OID in the SignerInfo block of a SignedData object, rather than the correct OID which is DSAwithSHA-1. Some receiving clients detected this anomaly, while others did not.

APPENDIX D
COMPANY CONTACT INFORMATION

Mr Charles Pierson
Baltimore Technologies
1310 Waterside
Arkington Business Park
Theale
Reading
Berkshire
RG7 4SA

Mr Andy Jepson
Compaq Computer Ltd
Worton Grange
Imperial Way
Reading
Berks
RG2 0TE

Mr John Hughes
Entegrity Solutions Ltd
23 Lomond Drive
Linsdale
Bedfordshire
LU7 7XH

Mr Ian Walker
Technical Director
Entrust Technologies Ltd
Apex Plaza,
Forbury Road
Reading
Berkshire
RG1 1AX

Mr Richard Parkinson
Product Marketing
Novell UK Ltd
Novell House
Arlington Square
Downshire Way
Bracknell
Berkshire

Mr Andy Campbell
Senior Consultant
Reflex Magnetics Ltd
31-33 Priory Park Road
London
NW6 7HP

Mr Paul Healy
RSA Security Inc
Fairfield House
Carey
Wokingham
Berkshire
RG40 2NP

(Since the PKI and Secure Messaging Demonstrator RSA Security Inc have taken over Xcert)

Mr John Botting
Shym
400 Thames Valley Park Drive
Reading
Berkshire
RG6 1PT

Ms Allison Barnett
Spyrus UK Ltd
Regents Place
Suite 304
338 Euston Road
London NW1 3BT

Mr David Trevitt
SSE Ltd
Fitzwilliam Court
Leeson Close
Dublin 2
Rep. of Ireland