Final Report

A two-year project

fully-funded by the European Commission and
the Swiss Government

run by EEMA as part of a 13-strong management consortium

to solve the current interoperability problems associated with the deployment of Public Key Infrastructure (PKI) technology

www.eema.org/pki-challenge

The pkiC Management Consortium: -

Baltimore + Belgacom + Royal Mail + EEMA + GlobalSign + KPMG + Makra Security & Standards + SmartTrust + University of Leuven + University of Salford + Utimaco + WISeKey

An EEMA Project

The European Forum for Electronic Business

Funded by

European Commission

Swiss Government

Contents

1 Executive Summary

1.1 pkiC project overview

The pkiC is a PKI interoperability project that ran between January 2001 and April 2003. The pkiC has established a common framework whereby implementations of secure electronic commerce infrastructure and user technology from product suppliers, service providers, European projects and standard initiatives, can be linked together through practical interoperability trials.

The main objective defined at the project start was to establish such a framework for implementations to be linked together in trials to prove product interoperability. The practical experiences gathered during the execution of these trials can be used by other EU projects, initiatives and industry to further develop a comprehensive and cohesive solution for electronic commerce across Europe. A secondary objective is the promotion of practical solutions across Europe.

These objectives were reflected in the in the creation of the project consortium. The consortium members were technology vendors (Sonera SmartTrust, Entegrity[1], Entrust[2], Baltimore and Utimaco), service providers (Belgacom, GlobalSign, WISeKey), Academic Institutions, (University of Leuven, University of Salford), consulting companies (KPMG Information Risk Management, Makra, and Security & Standards) and a User Organisation (Royal Mail).

The work to be done for the pkiC was divided into 8 work packages:

- WP 1: Project management
- WP 2: Scope and definition of technical product /service interoperability criteria
- WP3: Identifying and contracting the participants
- WP4: Definition of the test plan
- WP5: Realisation of the test infrastructure
- WP6: Interoperability testing
- WP7: Demonstration and dissemination
- WP8: End-report

Each of the consortium members had clearly identified responsibilities within these work-packages.

1.2 Project achievements

Despite the organisational difficulties faced during the progress of the project (withdrawal of Entegrity and Entrust and the restructuring of Utimaco), the pkiC has achieved many of its goals.

About 15 testing participants showed their interest in the project and 10 of them have executed and reported at least a subset of the tests. These companies are: Baltimore Technologies, Cryptomathic, Guardeonic Solutions, Microsoft, RSA Security, Safelayer, TC TrustCenter, Sonera SmartTrust, UTI Systems and VeriSign. Short summaries of each of the participants (also the participants that haven't executed the tests) can be found in annex A.

[1] Entegrity decided to stop their pkiC activities in June 2001.
[2] Entrust decided to stop their pkiC activities in June 2001.

Each of the participants had access to the specially designed pkiC test website, hosted for the project by Royal Mail, to get access to the reference system and to upload their test results. The cross certification tests were designed in such a way that participants could execute the tests using automated protocols (Simple CMC and CMP). A manual process was also available as a backup. Knowing this, one of the most remarkable findings of the project was the fact that the majority of the participants executed their tests manually.

Besides interoperability problems, the pkiC also identified other issues that could cause significant problems in a security environment. These problems are related to directory systems and secure e-mail clients. Chapter 4 gives a deeper analysis of all the problems.

Details about the tests executed may be requested directly from the testing participants. Annex B contains the contact information for each of the participants.

1.3 Recommendations

Technical interoperability by means of cross certification between CAs can be achieved without real difficulties as proven in the trials. Nevertheless, a few basic rules need to be borne in mind to avoid trouble such as using a correct PKCS#10. Chapter 4 contains the detailed recommendations.

Besides this final overall report of the pkiC, three other documents have been produced that explain and explore the interoperability issues in greater detail:-

- Best practices for PKI users (D8.2)
- Recommendations for PKI vendors (D8.3)
- Challenges for the PKI Industry (D8.4)

1.4 Future of pkiC

All testing participants executed at least a basic set of the interoperability tests. The technical recommendations as specified in this document and in the “Best Practice” documents will be delivered to the different standardisation bodies.

The majority of the testing participants have expressed an interest in a new project to help them and the PKI industry in general to achieve more customer trust in PKI products. Some of the problem-areas identified during the pkiC are already under test in other initiatives such as S/MIME or CMP testing. A possible recommendation for a future project is the testing of PKI product requirements against the European Directive for electronic signatures and the particular country legislations related to this topic. Such a new project could act under the control of the new European “Sixth Framework Programme” (FP6).

2 Project organisation

2.1 Overview

2.1.1 Workpackages

Work-package number	Work package title
1	Project Management
2	Scope and definition of technical product/service interoperability criteria
3	Identifying and contracting participants
4	Definition of test plan
5	Realisation of test infrastructure
6	Interoperability testing
7	Demonstration & dissemination
8	End-report

Table 1: Workpackage list

2.1.2 Composition of the Consortium

The following table shows the composition of the pkiC consortium as originally constituted up until June 2001.

Participant name	Country	WP1	WP2	WP3	WP4	WP5	WP6	WP7	WP8
EEMA	UK			L				L	
KPMG	NL	Q							
Security & Standards	UK	PM							R
Entegrity	UK		L		R	R	R		
Belgacom	B		M				R		L
ID2	S		M				R		
Entrust	CH		M		L	M	M		M
Makra	UK		M						
University of Leuven	B		R						
University of Salford	UK		R						R
GlobalSign	B		R				R		
Post Office	UK				M	L	L		M
Baltimore	IE							M	
Utimaco Belgium NV	B	D							
Key: PM = Project Manager D = Director Q = QA Manager L = Leader of WP M = Member of WP R = Reviewer of WP									

Table 2: Original Consortium

The project overcame a major set back in June 2001 due to the withdrawal of Entrust from the consortium. Entrust were to have played a major role in pkiC, leading WP4 and as a major contributor to WP2, WP5 and WP6. Indeed, Entrust were going to supply the Reference Implementation, the heart of the testing infrastructure. The problems related to the withdrawal of Entrust were compounded by the subsequent withdrawal of Entegrity, which asked to withdraw from the consortium once WP2 was completed. Entegrity, having led the WP2 effort, which formed the technical basis for the remainder of the project, would have continued to provide the technical continuity as the reviewer of WPs 4, 5 & 6.

As the result of these events, the coordinator, supported by the project management team, rebuilt the consortium over the summer of 2001. However, contractual renegotiations and processing delayed the full restart of the project until April 2002. In the mean time, the WP2 work completed and a start was made on WP4, although severely restricted by commercial considerations concerning the progress of the new contracts.

The following name changes and company restructuring occurred during the lifetime of the project:

- Post Office to Consignia to Royal Mail (name change only)
- ID2 to Sonera SmartTrust
- Utimaco Belgium NV to Utimaco AG

The following table shows the composition of the pkiC consortium as rebuilt in July to September 2001.This composition was in operation as of April 2002.

Participant name	Country	WP1	WP2	WP3	WP4	WP5	WP6	WP7	WP8
EEMA (Coordinator)	UK			L				L	
KPMG	NL	Q							
Security & Standards	UK	PM							R
Belgacom	B		M				R		L
Sonera SmartTrust	S		M				R		
WISeKey	CH				M	M	M		M
Makra	UK		M						
University of Leuven	B		R						
University of Salford	UK		M/R						R
GlobalSign	B		R				R		
Royal Mail (Post Office, Consignia)	UK	D			L	L	L		M
Baltimore	IE							M	
Utimaco AG (Utimaco Belgium NV)	B				M	M	M		M
Key: PM = Project Manager C = Coordinator Q = QA Manager L = Leader of WP M = Member of WP R = Reviewer of WP									

Table 3: Rebuilt Consortium

2.1.3 The main achievements of pkiC

The main achievements of pkiC were to:

- achieve a good level of testing by 10 Testing Participants
- identify clearly the major causes of PKI lack of interoperability
- make good presentations and effective demonstrations at EEMA 2002 and ISSE 2002
- increase the awareness of PKI in Europe and beyond

Another achievement to be mentioned is the strong project management needed to overcome the various delays caused by the withdrawal of Entrust and Entegrity in June 2001 and then the restructuring of Utimaco NV.

2.2 Project objectives

Due to the restructuring of the consortium and the consequential delays to pkiC, the nature of the project inevitably changed. Section 2.2.1 describes the initial project objectives. The forced project changes led to a modification of the project objectives, as outlined in section 2.2.2.

2.2.1 Initial Objectives

The use of Internet and Internet based technologies for business as well as for private use is increasing rapidly. Nevertheless, business and consumers have been limited to only a fraction of potential capabilities of Internet-based technologies, especially in the area of secure electronic commerce and messaging. One of the barriers for the further development of electronic commerce over the Internet is the lack of practical interoperability between different IT Security technologies based on generally agreed standards.

In recent years, technologies and standards have been developed to enable integrity, confidentiality, identification and non-repudiation of e-commerce transactions. In addition, there are currently a number of European projects and initiatives under the 5th Framework as well as in other related IT programmes (e.g. EESSI, ISIS) that are establishing standards and implementing the enabling technologies for secure electronic commerce.

Regardless of how fast the growth of the Internet and the establishment of security standards is, the benefits of electronic commerce cannot be exploited fully by the European Community because of the lack of practical interoperability between electronic commerce enabling technologies such as Public Key Infrastructures (PKI). Only through an initiative that brings together the various standards based technologies through practical interoperability trials, can a truly European wide solution be established. Only by joining all the component parts of the secure electronic commerce "jigsaw" together, can the existence of a complete solution or deficiencies be determined.

EEMA[3]/ECAF proposed, with "pkiC", the establishment of a test framework that would permit heterogeneous implementations of secure electronic commerce technologies, from product suppliers, service providers, European projects and standards initiatives, to be linked together for the purpose of practical interoperability trials. The experience of the trials and the lessons learned would enable EU projects, initiatives and industry to further develop

[3] EEMA is the *European Forum for Electronic Business*, a non-profit association with currently 230 members from all over Europe. ECAF, *European Certification Authority Forum*, is an Interest Group within EEMA

towards a comprehensive and cohesive solution for secure electronic commerce across Europe.

The subjects of the trials in the pkiC where wide-ranging and included:

- Public Key Infrastructure (PKI) technologies,
- Certification Service Providers (CSPs) including Certificate Authorities,
- Security enabled client applications, which use PKI technologies and CSPs to secure the most popular electronic commerce and electronic business applications (e-mail, web, EDI).

A secondary but nevertheless important objective was to promote the existence of practical solutions for Secure Electronic Commerce integrated across Europe.

The pkiC's objectives were to be achieved through the realisation of the following:

- Interoperability testing between Public Key Infrastructures of participating vendors/users/European projects, CA service providers, and PKI client applications of participating vendors/users/European projects. This was on the basis of well-established standards (e.g. X.509v3, PKIX), EU laws (e.g. the "EU Directive on Electronic Signatures") and the associated EESSI (the European Electronic Signature Standardisation Initiative), projects (e.g. the FP4-funded projects) and best practice (e.g. EEMA's Secure Messaging Framework).

- Demonstration and dissemination of the results of the former objectives at ideally two major European Electronic Commerce Events: "ECE2002" (EEMA's Annual Event – see www.eema.org) and "ISSE2002" (.eema.org/isse), depending on the start date of the Challenge.

The interoperability issues that were to be tested in this challenge are outlined in the (simplified) picture below.

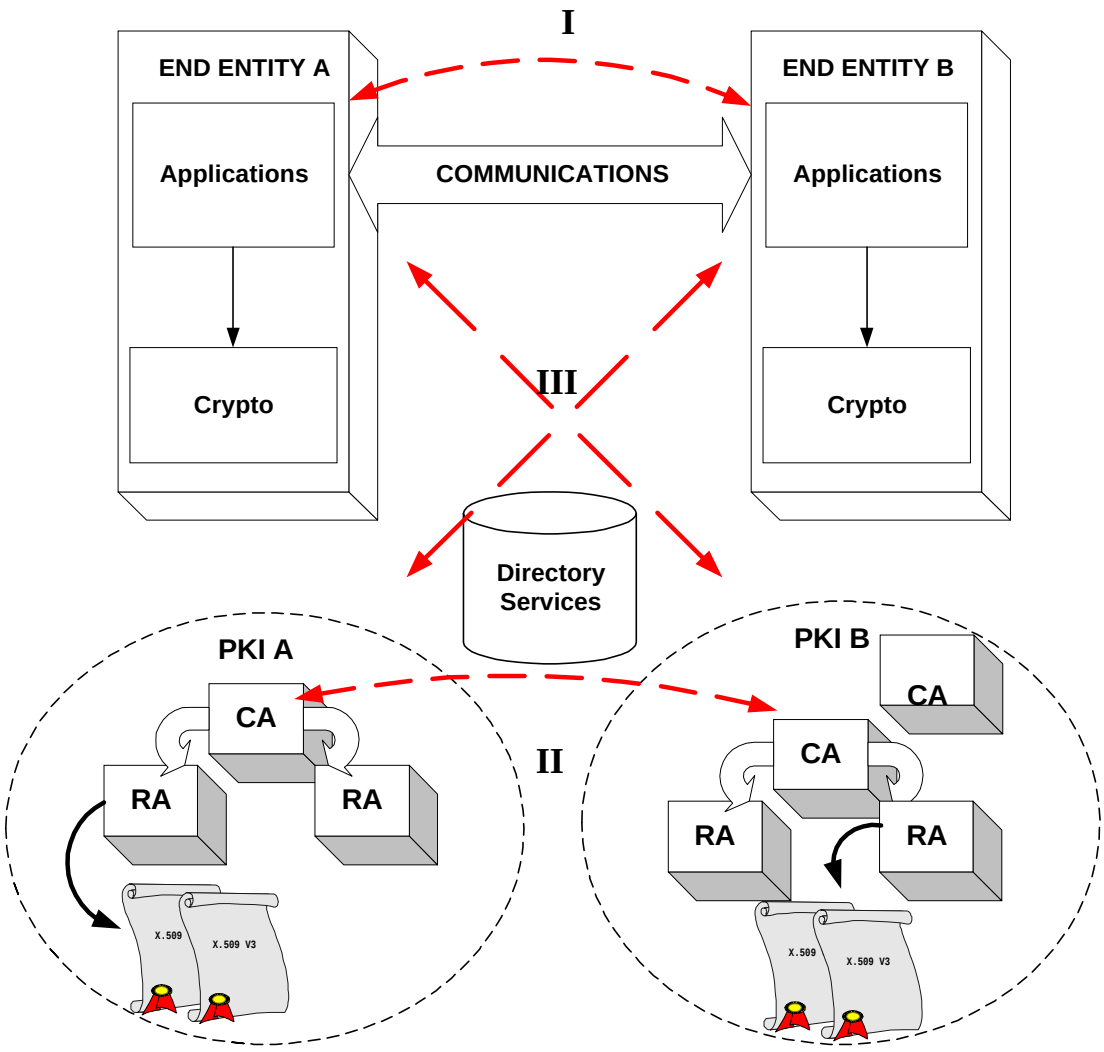

Figure 1: Interoperability issues tested in pkiC

The pkiC project was to provide a tool to prove the interoperability of innovative solutions in at least the following potential areas:

- At the most basic level the ability for applications to exchange and operate with each other's certificates;
- In multiple PKI scenarios, the use of cross certification and/or user trust lists;
- The use of certificate revocation solutions;
- The use of supporting trust services for non-repudiation such as time stamping (if not too early for this) and timed audit logs;
- The use of cryptographic techniques for digital signatures and confidentiality;
- The use of qualified certificates in support of qualified signatures for the Electronic Signature directive;
- The possible use of attribute certificates;
- The use of smart card technologies.

The project examined the practical aspects of the possibility for proving interoperability in at least these areas when deciding the criteria for the acceptance of products and services for the pkiC. The support for certain technologies (e.g. PKIX) was mandatory and for others (e.g. time stamping, smart cards) was optional.

2.2.2 Modified Objectives

As a consequence of the delays, the project changed the emphasis of the demonstration at EEMA 2002 to demonstrate the work to date and the demonstration at ISSE 2002 also had to be changed at a very late stage as the actual test results were not available. In addition to this the iterative process of testing, bug fixing and regression testing originally planned could not take place across all the testing participants. Some did find bugs and were able to retest their fixed implementations to a limited extent. The nature and scope of the Final Report therefore has changed to concentrate on these positive results as follows:

- A range of causes of failure to interoperate were discovered; and
- The Reference Implementation became robust and represented a correct implementation of the profiles of the standards as specified in D2.2 Product/Service Interoperability Criteria.

The consensus amongst the testing participants is that pkiC could justifiably claim success for these reasons alone.

The actual number of testing participants fell due to the delays, in part since some were not ready in time, but also the nature of the market had changed significantly during the two years since the inception of the project leading to poor trading conditions. The list of the 10 testing participants is given below:

- Baltimore Technologies
- Cryptomathic
- Guardeonic Solutions
- Microsoft
- RSA Security
- Sonera SmartTrust
- Safelayer Secure Communications
- TC TrustCenter
- UTI Systems Romania
- VeriSign inc.

2.3 Project management and co-ordination aspects

2.3.1 Methodologies

Two methodologies were used on this project:

- Interoperability testing against a Reference Implementation
- The use of Prince 2 project management techniques

Generally, there are two recognised methods for conducting interoperability tests. One, adopted by pkiC, is where all the Testing Participants test their products and services against a Reference Implementation. The other is to conduct pair wise testing amongst the population of products. The primary reason for choosing the Reference Implementation approach was cost and management control. For 10 Testing Participants, only 10 test

campaigns were needed with a Reference Implementation approach. For pair wise testing, some 45 test campaigns would be needed. Also, by using the Reference Implementation approach it would be possible to enforce compliance against a single specification. The main objection to the pkiC approach is the assertion that, if products A & B interoperate against a Reference Implementation, it does not guarantee that product A will interoperate against product B.

The two approaches are clearly complementary and the original plan for pkiC was to encourage pair wise testing amongst the Testing Participants once Reference Implementation testing was complete. Unfortunately, time was not available to do this. Nevertheless, it should be noted that the UK initiative by CESG (see www.cesg.gov.uk/publications/index.htm) took the pair wise testing approach and it was this that encouraged both projects to collaborate since the approaches were seen as being complementary.

On the management front, it was decided to make use of Prince 2 techniques in a lightweight fashion. Prince 2 is perceived to be an effective project management methodology and is in widespread use throughout UK Government departments. See www.ogc.gov.uk/prince.

2.3.2 Major Disruption to the Project

pkiC suffered major disruption due to key consortium members either pulling out or being restructured. Consequently, the original aims of the project were compromised. This section gives a short analysis of the situation.

The kick-off meeting for the project took place on 2001/01/31 in Brussels. Although slightly late the project got off to a good start and quickly regained lost ground. A project meeting was due to take place at Entrust in Zürich on 2001/06/20. However, earlier in that month, Entrust informed the project that its Zürich operation would be subject to immediate closure with the loss of all the related jobs. Although Entrust did indicate that it would fulfil its obligations in relation to WP2, in the end this did not occur. Soon afterward the project was informed that Entegrity would also be withdrawing from the project after the completion of WP2. In the event, WP2 had to be extended beyond 2001/06/30 and with the assistance of the University of Salford, the document was completed towards the end of 2001.

The project was structured so that Entrust, having completed its WP2 work, would lead the WP4 effort (Test Specifications), move on to implement the Reference Implementation in WP5 based on its own product set and go on to support the testing in WP6. The demise of the Entrust Zürich operation was clearly a body blow to the project. In addition, Entegrity would have participated in the remainder of the project in order to provide continuous support in the role of Technical Authority. The exit of Entegrity was therefore also a major setback for the project.

Rather than request termination of the project, the management decided to attempt a consortium reconstruction. By September 2001, the Swiss Company WISeKey had agreed to join the project to take up a part of the Entrust responsibilities (all apart from the Reference Implementation) and Utimaco, an existing consortium member agreed to provide the Reference Implementation. The Royal Mail took over the management of WP4 and WP5, and provided a substitute Project Director. Some of the budget allocations were adjusted. Negotiations on a new contract with the Commission started but these were not completed until March 2002. In the mean time both WISeKey and Utimaco agreed to start work at the

beginning of 2002 but only at a relatively low level of activity pending the signing of the new contracts. A major delay in the project was clearly inevitable

The initial project plan showed testing taking place between January and June 2002. The intention was for the Testing Participants to perform their initial testing against the Reference Implementation in order to identify bugs in their implementations and possible bugs in the Reference Implementation. The Testing Participants could then fix the bugs and return to perform the actual tests against the Reference Implementation. There should have been sufficient time for this iterative process to complete, with the bulk of implementations achieving complete interoperability by June 2002. If possible there would be additional time to perform pairwise testing. The timing was such that presentations and displays could have reflected the success of the testing at both EEMA 2002 and ISSE 2002. The final report would then be able to reflect the successful achievement of interoperability across a range of products.

However testing did not start until August 2002 during which a number of pilot tests were performed. The project was confronted with a large number of bugs in the Reference Implementation and at the beginning of October 2002, at a critical moment in the project; Utimaco's operation in Belgium was restructured. Utimaco AG, the parent company took over the responsibilities in relation to pkiC and employed the main person supporting the Reference Implementation. However, further delays to the project occurred as the restructuring of Utimaco took effect. The actual testing phase was delayed until mid-October 2002 and carried on until mid-December 2002. In the mean time, the project had been granted an extension until the end of 2003/02/28; a further extension until the end of 2003/04/31 was granted to enable the European Commission's request for three best practice documents to be written.

2.4 Deliverables and References

Apart from the various management reports to the Commission of the European Union and this report, a small number of key deliverables were published. These were:

- D2.1 The EEMA Inter-organisational Message Security Framework
- D2.2 Product/Service Interoperability Criteria
- D4.3 Final Test Plan

In addition to these written deliverables, the other major deliverable was D5.1 Test Infrastructure.

2.4.1 D2.1 The EEMA Inter-organisational Message Security Framework

This is one of three documents published by EEMA that deal with the provision of a class of Secured Information Interchange Applications (known as SII) that use Public Key Infrastructures, Public Key Cryptosystems and X.509 Certificates to protect the interchange of electronic information between individuals and between organisations. The documents are:

- A **Memorandum of Understanding (MoU)**, which establishes agreements on the business semantics of a set of Security Functions that are provided to users to allow them to create, protect and assess the trustworthiness of information. It contains a Signature Policy and rules for binding digitally signed information with its originator and the MoU. It also establishes a business and user understanding of the

commitments they make when they invoke the Security Functions. The MoU is therefore a multilateral agreement to the use of the Security Functions. A reference to the MoU is contained and signed by users and user organisations in each message, document or information object interchanged according to SII to indicate their exact intentions in creating secured information and binding to it by applying digital signatures. The MoU will therefore primarily be of interest to the user community;

- A **Framework**, which contains technical specifications or references to technical specifications for inter-working at various levels to ensure that SII systems and services that create, transfer, receive and use secured information can properly support the Security Functions specified in the MoU. The MoU references the Framework. It is of primary importance to those who intend to implement the security functions (i.e. product suppliers) and the PKI supporting it, and those who need to assess the security provided by the Framework (e.g. an organisation's internal security department);

- A **Guide, which explains further** the Framework and the MoU. The Guide contains notes and guidance on the MoU and the Framework for implementers and users. It is of a more tutorial nature, and will primarily be of use to those in organisations responsible for establishing SII applications.

2.4.2 D2.2 Product/service interoperability criteria

The objective of this document is to specify the interoperability testing criteria for the pkiC. It defines the scope and the criteria for interoperability for PKI products and services. It is against these criteria that products and services were selected for the interoperability trials.

The approach of D2.2 in specifying the interoperability criteria was to profile the various standards that have been developed by the industry over the past few years which form the technical basis for PKI products and services that are in the market place. In addition, D2.2 took into account the level of adoption of these standards in current products and services so that the interoperability criteria developed reflected what could be found in the market place. In this way, the pkiC was sure that product suppliers and service providers were in a position to put forward their wares for testing. This approach enabled D2.2 to specify a range of standards profiles that provide values for various options that were left open in the standards.

2.4.3 D4.3 Final test plan

This deliverable is in 5 parts:

- Part 0 - D4.3.0 Guide to Preparation & Testing
- Part 1 - D4.3.1 Test Plan for Cross Certification
- Part 2 - D4.3.2 Test Plan for Subordinate CA Certification
- Part 3 - D4.3.3 Test Plan for Enrolment
- Part 4 - D4.3.4 Test Plan for Certificate Validation

In addition there is a specification that was not part of the original deliverables but nevertheless is a useful document. It is designated as:

- Part 5 - D4.3.5 Web Test Management Interface Specification

2.4.4 D5.1 Test Infrastructure

Formally, this deliverable was the test infrastructure itself. However, it was decided to make the following document available:

- D5.1 Description of Reference System

2.5 Presentations at conferences and articles

Apart from the planned activity at EEMA 2002 in London and ISSE 2002 in Paris, members of the consortium presented the pkiC at a number of conferences and events.

A full list of the events where the pkiC has been presented can be found in Annex D.

Also, in addition to the planned pkiC Web site www.eema.org/pki-challenge activity, Updates sent to interested parties and articles were placed in EEMA Briefing and Online, a number of cross references were made to the pkiC Web site from other Web sites and a number of articles were written.

2.6 Press Coverage

Annex E contains a sample of the press coverage achieved by the project.

3 Tests

3.1 Test preparation

3.1.1 Testing areas

The structure of the tests is described fully by the documentation created by Work Package 4. These in turn follow closely the interoperability model developed by Work Package 2. For convenience the tests and the interfaces are described here briefly.

The interoperability tests exercise four interfaces in an idealised PKI model;

- Interface 1 - Cross certification between peer CAs
- Interface 2 - Subordination from a superior CA to a subordinate CA
- Interface 3 - Enrolment from a client to a CA
- Interface 4 - Validation of the status of a certificate by a client

These interfaces map directly onto the set of tests that have been designed to exercise the Interfaces;

- Test Group 1 – Cross Certification
- Test Group 2 – Subordination
- Test Group 3 – Enrolment
- Test Group 4 – Certificate Validation

The Test Groups themselves are structured to reflect the manner in which each process can be accomplished:

Test Group 1 consists of:

- Manual Cross-certification
  - Reference CA certifies Participant CA
  - Participant CA certifies Reference CA
- On-line Cross-certification using Simple CMC
  - Reference CA certifies Participant CA
  - Participant CA certifies Reference CA

Test Group 2 consists of;

- Manual Subordination
  - Reference Root CA certifies Participant Sub CA
  - Participant Root CA certifies Reference Sub CA
  - Reference Sub CA certifies Participant Sub Sub CA
  - Participant Sub CA certifies Reference Sub Sub CA
- On-line Subordination using Simple CMC
  - Reference Root CA certifies Participant Sub CA
  - Participant Root CA certifies Reference Sub CA
  - Reference Sub CA certifies Participant Sub Sub CA
  - Participant Sub CA certifies Reference Sub Sub CA

Test Group 3 consists of;

- Manual Enrolment
  - From Reference System to Participant CA**
  - From Participant Client to Reference CA
- On-line Enrolment using Simple CMC
  - From Reference System to Participant CA**
  - From Participant Client to Reference CA

Test Group 4 consists of;

- Testing for certificate Expiry
- Testing for certificate revocation
  - Through CRLs
  - Through OCSP

**Not implemented

Time constraints also precluded the implementation of some of the tests specified in the original project plans.

- CMP Cross-certification using MACs
- CMP Cross-certification using Signatures
- CMP Subordination using MACs
- CMP Subordination using Signatures
- Enrolment using CMP

3.1.2 Success and Failure

Time constraints played a significant role in the implementation of Test Group 4. The original specification for on-line support could not be met so the team assembled a limited tool that could be used for straightforward OCSP scenarios.

The pkiC Interoperability Web Site at Royal Mail contained a section that allowed the Testing Participants to upload the Test Results. As part of the upload they should also have selected whether the tests were successful or not. Everyone who uploaded results deemed them successful. This is debateable. The interoperability tests can be viewed as a two-stage process. The first stage involves the creation of a trust relationship while the second is the testing of that trust relationship through the mutual exchange of secure e-mail. Judging whether the first stage was successful was straightforward; either a CA successfully processed the request for trust or it did not. The measure was whether the appropriate Certificate was returned and that it contained the correct values. This was the measure that the test team felt had been applied by most of the Testing Participants. While superficially weak it was valid because the second stage of the test process, proof of trust, was very difficult in practice to manage because of the technical inadequacies of the e-mail clients being used to exchange signed e-mails. That is not to say that this area was a complete failure, but the inconsistencies in the behaviour of supposedly S/MIME compliant e-mail clients made it difficult to get consistent test results from different Testing Participants. See further comments on e-mail client behaviour in section 4 below.

3.2 Testing method

The central component of the interoperability tests was the Reference System. Created to comply with a predefined and agreed set of performance characteristics, themselves

constructed from widely agreed international standards. This chapter gives a brief technical introduction of how the reference system was organised.

3.2.1 Physical Structure

The pkiC Reference system was built and operated at Royal Mail's offices at Chesterfield in the UK. It consisted of a set of five servers. The CAs, RAs and supporting LDAP directory were installed on four Windows 2000 servers while the pkiC Interoperability Web Site that supported the test process ran on a Linux server. There was also a mail server and an Internet Gateway that hosted a firewall. There were a further three client devices that were used to host e-mail clients and test users. All these devices were located in the Royal Mail Research and Consultancy Group test area, behind the firewall and independent of the remainder of the Royal Mail network and communications infrastructure.

The following diagram illustrates the physical structure of the devices that comprised the Reference system.

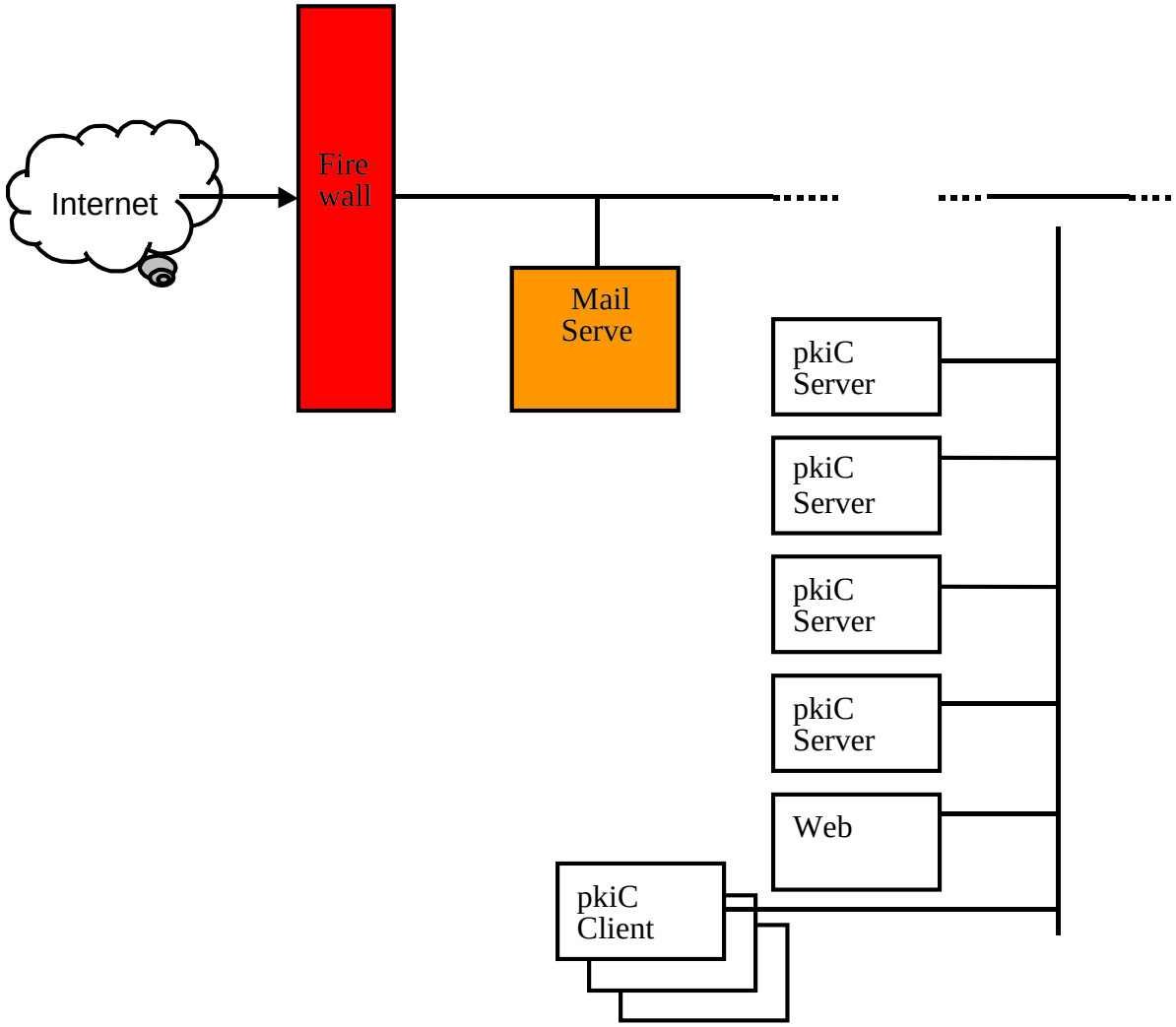

Figure 2: Physical structure of the pkiC Reference System

3.2.2 Logical Structure

The logical structure of the CAs in the Reference System is described in document D2.2 Interoperability Test Criteria. The entire structure, complete with RAs and End Entities is presented here.

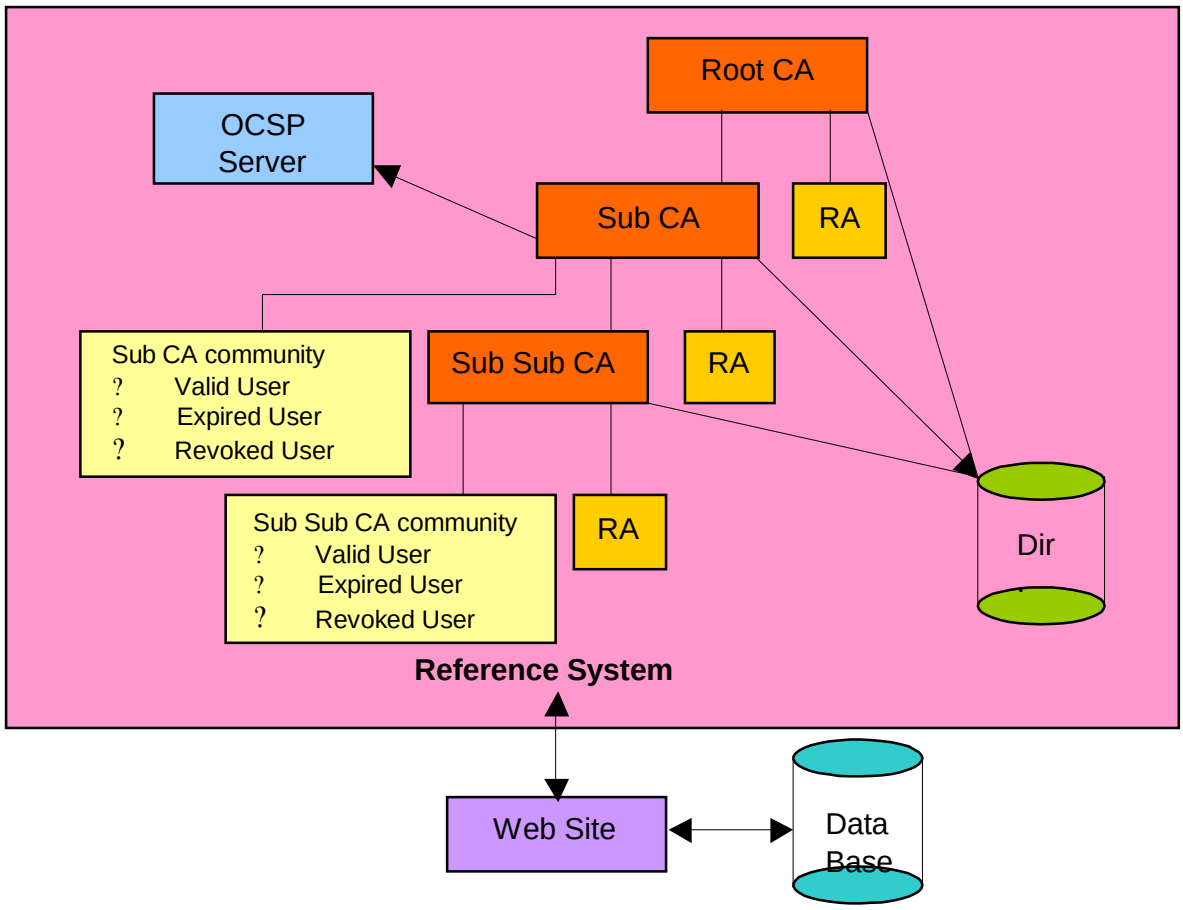

Figure 3: The logical structure of Reference System and Web Site

The relationship between the physical servers and the logical components was as follows:

- pkiC Server 1 – Root CA, Root RA
- pkiC Server 2 – Sub CA, Sub RA
- pkiC Server 3 – Sub Sub CA, Sub Sub RA
- pkiC Server 4 – Mercury Mail Server, Directory, OCSP Server
- pkiC Server 5 – pkiC Interoperability Web Site

3.2.3 Technical Specifications

The model and version numbers for each of the components in the system was as follows:

Component	Manufacturer/Product/Version
Servers	Compaq Proliant 1850R
PKI software	Specialised version of Safeguard from Utimaco AG
Hosting Operating system for PKI software	Windows 2000 5.00.2195 with Service Pack 2
Web site software	PHP v4.2.2
Hosting Operating System for web site	Linux v7.2 from Red Hat
Supporting database for pkiC Interoperability web site	MySQL v3.23.49
e-Mail service for end users	Microsoft Exchange Enterprise Server 2000 with Service Pack 3
e-Mail service for CMC enrolment	Mercury/32 v3.31
OCSP Service	Sytrust CertControl v1.2
Firewall	Checkpoint Firewall 1 NG with Feature Pack 2
Directory Service	OpenLDAP v1.8.8.7
Web Server	Apache v1.3.20
Client Devices (3)	Compaq Deskpro
Client Device Operating System	Windows 2000 5.00.2195 with Service Pack 1

Table 4: System Components

The three client devices used at Royal Mail were installed with e-mail clients of various manufacturers and/or types throughout the testing in the proof-of-trust stage of the tests. At one time or another the test team used the following:

- Microsoft Outlook 2000
- Microsoft Outlook Express version 5
- Microsoft Outlook Express version 6
- Microsoft Outlook 2000 + Utimaco Sign&Crypt Plug-in v3.0.2
- Eudora Pro v4.0
- Lotus Notes v5.0.5

3.2.4 Supporting Services

3.2.4.1 e-Mail service and e-Mail accounts

The Reference System used two separate e-mail systems. For on-line enrolment the system used a Mercury mail server residing on the same machine as the directory server. Each of the CAs in the Reference System had an account with the Mercury server. e-Mails for CMC enrolment were forwarded to the CAs from here. e-Mails back to the enrolees were sent via the Royal Mail Research and Consultancy Services Test Area Exchange e-mail server. For the proof of trust through e-mail exchange, end users both within and outside the Reference community used the Royal Mail Research and Consultancy Services Test Area Exchange e-mail server. Where necessary, e-mail accounts were created for users from the Participants communities to aid the testing process.

3.2.4.2 Firewall

The Reference System was protected by the Royal Mail Research and Consultancy Services Test Area firewall. The rules governing access permissions and authorisation were built into the firewall, allowing through only those people with explicit authority to access the Reference System.

3.2.5 Access Control

Access to the web site that acted as a front-end to the Reference system was controlled through filter rules in the Royal Mail firewall. The pkiC system administrators were responsible for creating and maintaining the filter rules in the firewall that permitted access from IP addresses submitted by the Testing Participants. An extra level of User ID-based security built into the web site itself required all end users to register with the system and create private web site accounts.

Once logged into the system the Testing Participants navigated to the section in the web site that described the network information for the machines on which their own PKI software was running. The forms were completed on-line and the information submitted to the web site whereupon they were given access to the remainder of the system by the web-site administrators.

A further level of access control was provided by the enforcement of SSL between the web site server and the clients performing the tests.

3.2.6 LDAP Directory Support

The pkiC was undertaken in the knowledge that it could be compromised by the long-established issues that the PKI industry has with the inconsistent use of LDAP directories by PKI software. The X.500 attributes used to store PKI items such as Certificates and CRLs have more than one accepted method of naming them (i.e. either with or without the *binary* description). In addition they have no consistent location within the Directory Information Tree and the precise structure and location is vendor dependant. This was a serious problem because LDAP servers cannot yet support searches for particular certificates and CRLs. Taken together, this means that it is highly unlikely that a vanilla implementation of PKI software from one vendor would be able successfully to query the LDAP directory of another. This problem is compounded further by the fact that the basic structure for X.509

certificates[4] does not carry in it any information that allows relying software to locate either the publishing CA[5] or the directory that supports it.

The pkiC employed two techniques to mitigate these problems.

3.2.6.1 Mitigating the inability to search

The inability of LDAP servers to support the searching for PKI attributes, and the inconsistent use of the directory structure by different PKI vendors, was mitigated by the use of a pre-agreed and publicised directory schema. Support for the following Structural Objects was mandated:

- Country Name (C=)
- Location (L=)
- Organisation (O=)
- Organisational Unit (C=)
- Common Name (CN=)

In addition to this it was mandated that the Certificate Authority support the following attributes:

- cACertificate
- userCertificate
- authorityRevocationList
- certificateRevocationList

It was also recommended that the CA support:

- crossCertificatePair

All participants in the test phase were expected to implement this schema.

3.2.6.2 Lack of locator information in certificates

To mitigate the potential lack of locator information in the certificates the pkiC used a virtual directory that acted as a single point of contact for all directory enquiries. This service was provided by MaxWare of The Netherlands who had made available an instantiation of the MaxWare Virtual Directory (MVD) at their offices. This MVD acted as a proxy for all LDAP queries from pkiC Testing Participants.

[4] The AIA and CDP extensions carried locator information
[5] Microsoft DNs carried a DC component which described the location of the CA within the Microsoft network

The picture below gives an overview of the Directory services in write mode.

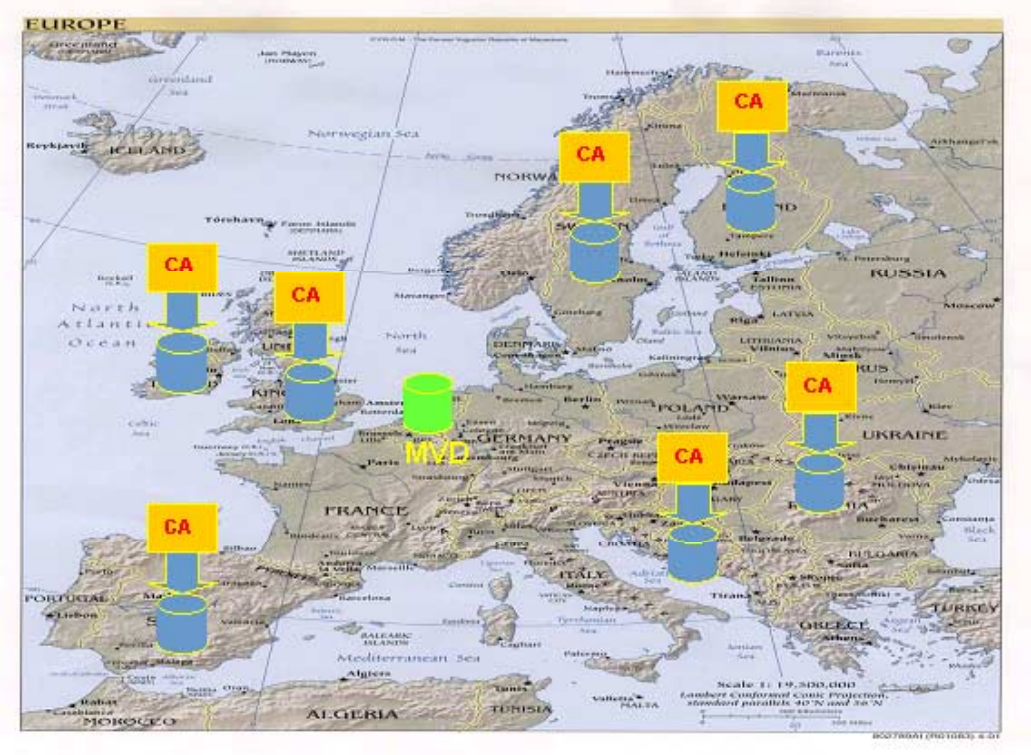

Figure 4: Directory services in 'write' mode

When participant CAs published PKI objects they wrote immediately to their own directory, locally and without reference to the MVD.

The picture below gives an overview of the Directory services in query mode.

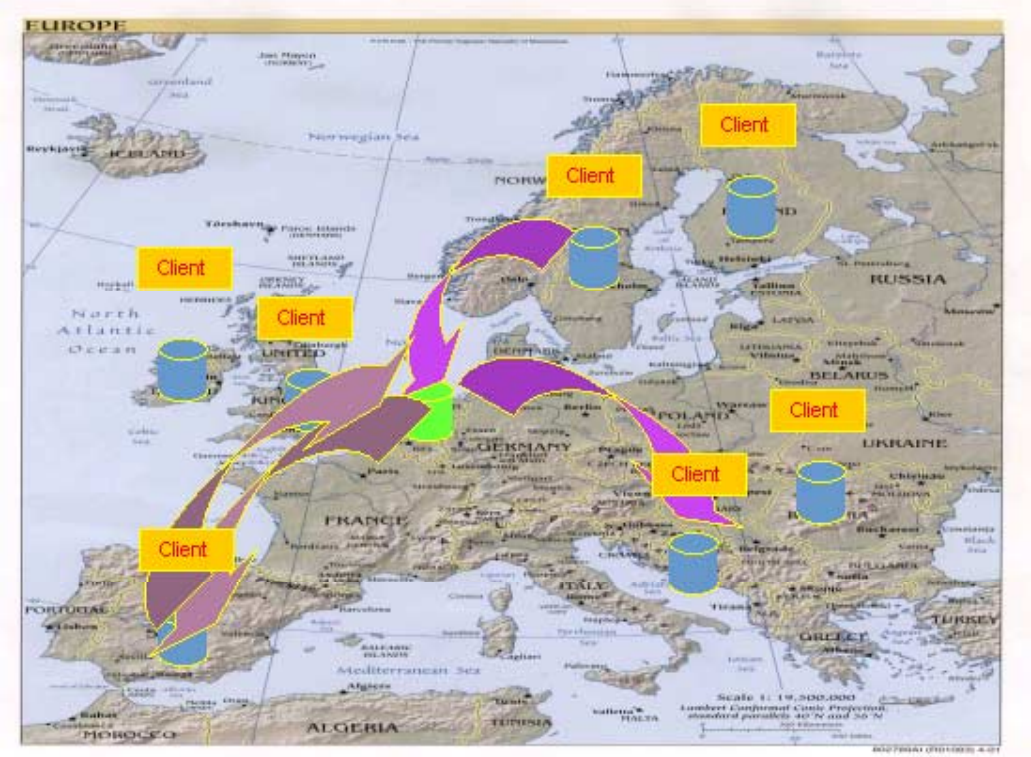

Figure 5: Directory services in 'query' mode

All enquiries by LDAP enabled clients were made through the MVD. The MVD used the DN in the enquiry to map the query to the physical server on which the object being sought resided. e.g. A query to recover the caCertificate from the Reference System Root CA specified a DN of C=GB, L=Chesterfield, O=Consignia, OU=PkiC Root CA. The C=GB, L=Chesterfield components of the DN in the query were enough for the MVD to identify that it be redirected to LDAP://62.189.12.27:389.

It should be noted that this query mode applied to all client software in the project. This meant that queries to the participant's ***own*** LDAP directory were also made in this way. This gave consistency of operation across the entire project.

3.3 pkiC Interoperability Web Site at Royal Mail

The pkiC Interoperability Web site was designed and built to reflect as accurately as possible the structure of the tests themselves. Following successful registration with the web site the Testing Participants were granted access to the parts of the Web site that supported the tests that they wished to perform. For a fuller description of the structure and operations of the pkiC Interoperability Web site see document D5.1 Description of Reference System.

Various control screens of the PKI Interoperability Website that were developed for the Test Groups are shown below.

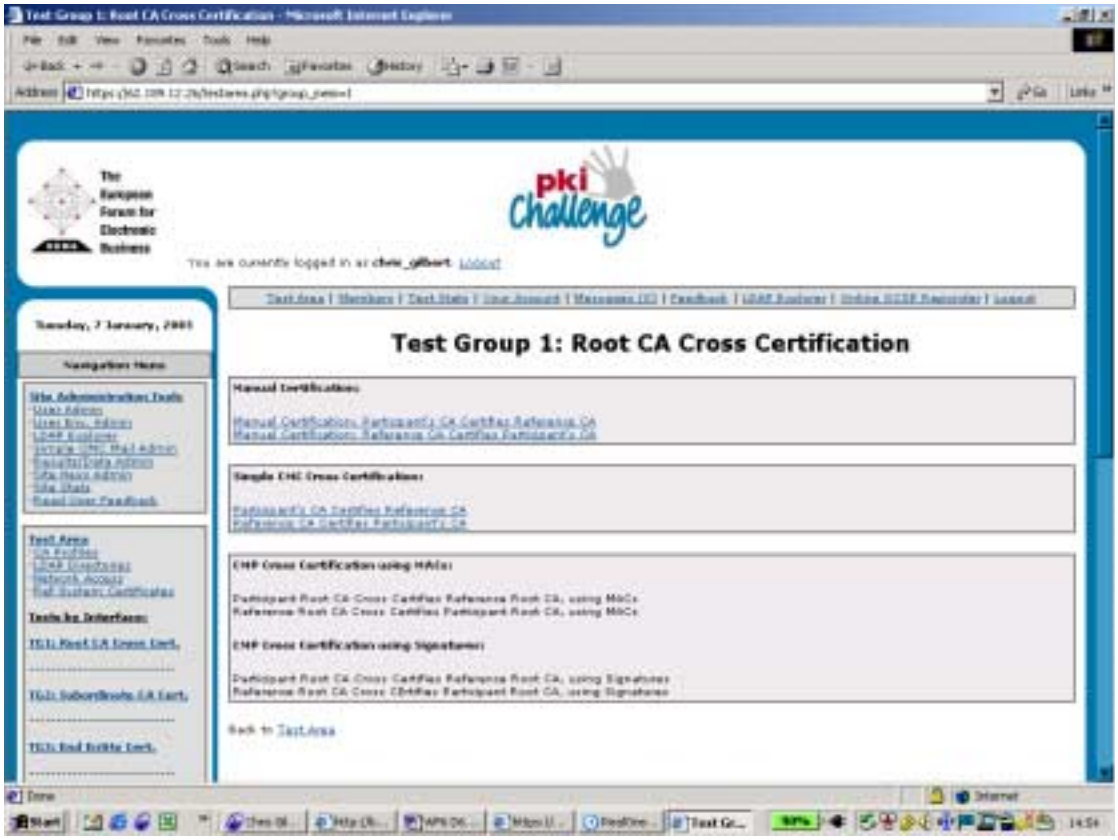

Figure 6: Control screen for Test Group 1

Figure 7: Control Screen for Test Group 2

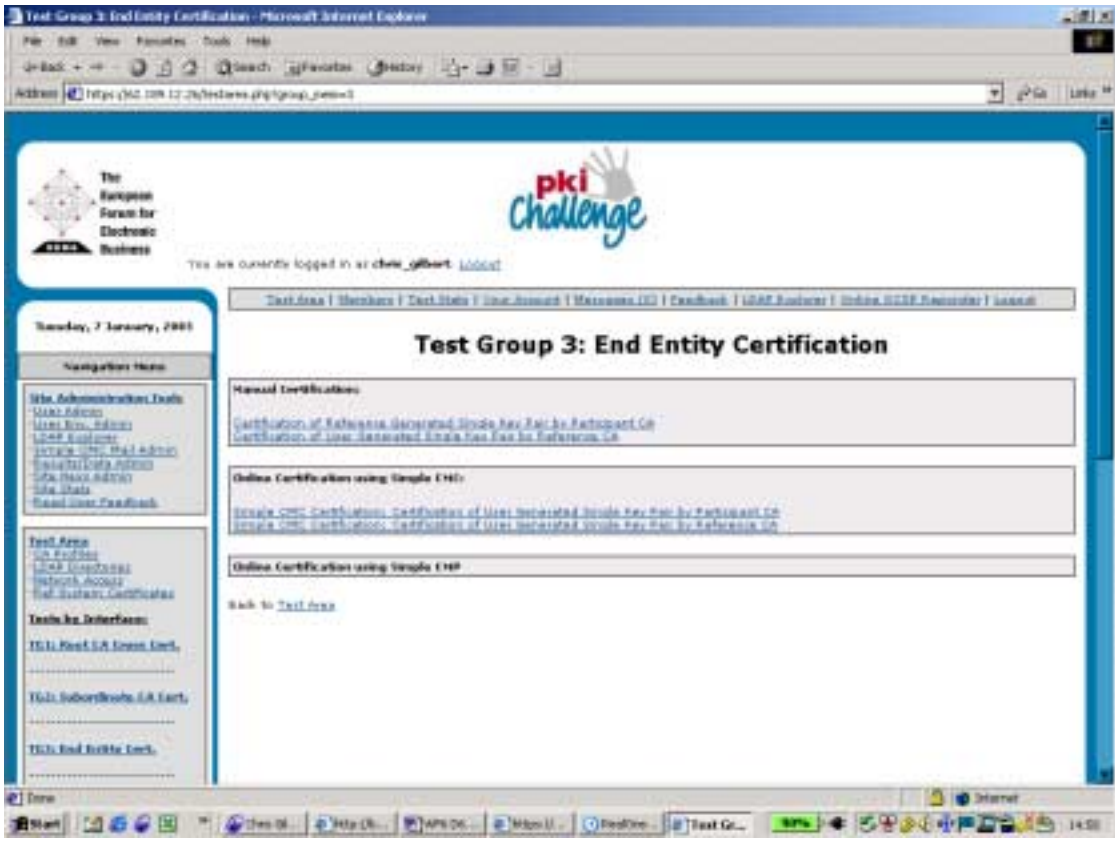

Figure 8: Control screen for Test Group 3

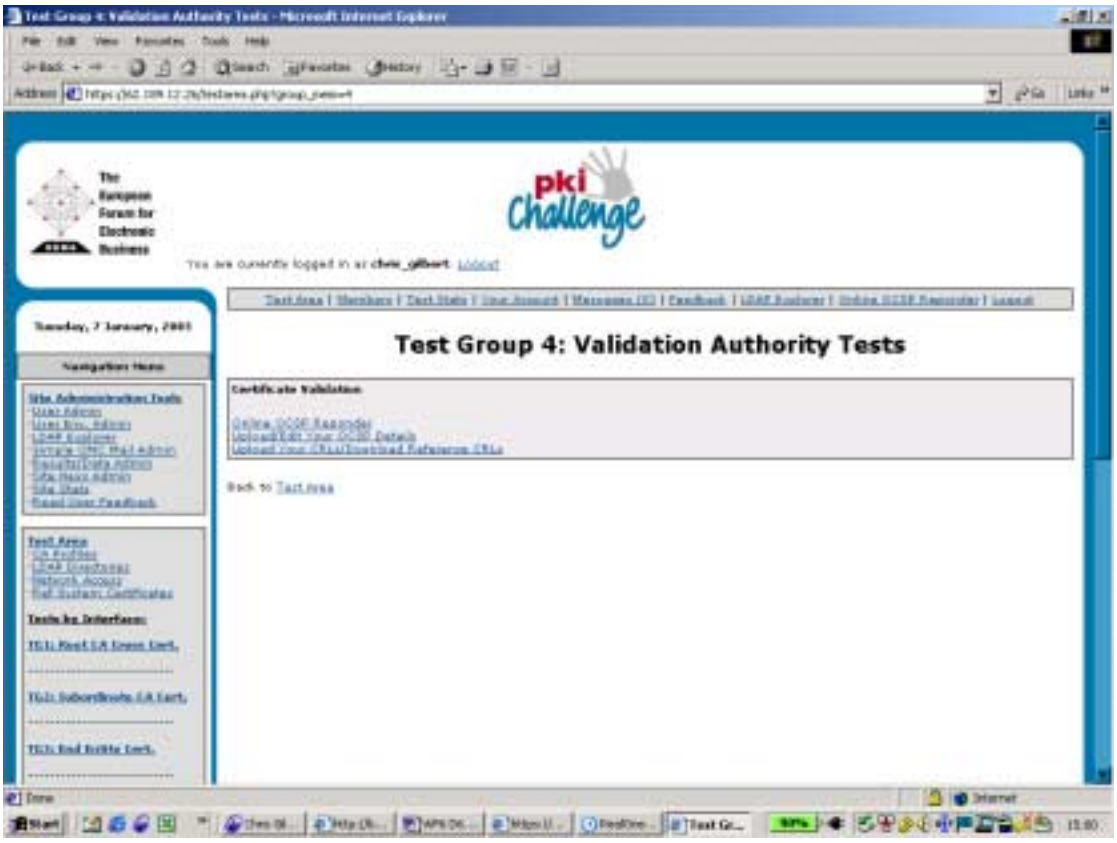

Figure 9: Control screen for Test Group 4

Behind each of these screens were the dialogues that allowed the Testing Participants to conduct the tests. The Web site had been built so that PKCS#10[6] submissions were processed automatically and did not require the intervention of the site administrator. PKCS#10s were uploaded to the site by the Testing Participants and inserted into the underlying database. The Reference System RA Batch programs monitored the contents of the database and picked up the new requests and submitted them to the CAs. The certificates were either returned automatically to the enrolee or posted to a place on the web site from where they could be downloaded.

CMC submissions had to be inserted manually by the system administrator using the Simple CMC Mail Admin option on the navigation bar to the left of the screen.

3.4 Testing statistics

The following test statistics are based on the results uploaded by the participants to the pkiC Web site or other written reports from the participants. Independent from these results, a small number of the participants tested against the reference system without reporting and these results are not included in the statistics.

[6] PKCS#10 is a PKCS#10 file – a file containing a request for a certificate

3.4.1 Executed tests

In total, 51 tests were reported. The following table shows in more detail which tests were executed.

TG	Test	Test description	Total
1	1	Manual Certification: Participant Root CA Cross Certifies Reference Root CA	11
	2	Manual Certification: Reference Root CA Cross Certifies Participant Root CA	7
	3	Simple CMC Cross Certification: Participant's CA Certifies Reference CA	2
	4	Simple CMC Cross Certification: Reference CA Certifies Participant's CA	1
	5	CMP Cross Certification using MACs: Participant Root CA Cross Certifies Reference Root CA	0
	6	CMP Cross Certification using MACs: Reference Root CA Cross Certifies Participant Root CA	0
	7	CMP Cross Certification using Signatures: Participant Root CA Cross Certifies Reference Root CA	0
	8	CMP Cross Certification using Signatures: Reference Root CA Cross Certifies Participant Root CA	0
Test group 1 total			**21**
2	1	Manual Certification: Participant Root CA Certifies Reference Subordinate CA	4
	2	Manual Certification: Reference Root CA Certifies Participant Subordinate CA	6
	3	Manual Certification: Participant's Sub CA Certifies Reference Sub-Subordinate CA	4
	4	Manual Certification: Reference Sub CA Certifies Participant Sub-Subordinate CA	4
	5	Simple CMC Certification: Participant's Root CA Certifies Reference Sub CA	1
	6	Simple CMC Certification: Reference Root CA Certifies Participant's Sub CA	1
	7	Simple CMC Certification: Participant's Sub CA Certifies Reference Sub Sub CA	1
	8	Simple CMC Certification: Reference Sub CA Certifies Participant's Sub Sub CA	1
	9	CMP Certification using MACs: Participant's Root CA Certifies Reference Sub CA	0
	10	CMP Certification using MACs: Reference Root CA Certifies Participant's Sub CA	0
	11	CMP Certification using MACs: Participant's Sub CA Certifies Reference Sub Sub CA	0
	12	CMP Certification using MACs: Reference Sub CA Certifies Participant's Sub Sub CA	0
	13	CMP Certification using Signatures: Participant's Root CA Certifies Reference Sub CA	0
	14	CMP Certification using Signatures: Reference Root CA Certifies Participant's Sub CA	0
	15	CMP Certification using Signatures: Participant's Sub CA Certifies Reference Sub Sub CA	0
	16	CMP Certification using Signatures: Reference Sub CA Certifies Participant's Sub Sub CA	0
Test group 2 total			**22**
3	1	Manual Certification: Certification of Reference Generated Single Key Pair by Participant CA	0
	2	Manual Certification: Certification of User Generated Single Key Pair by Reference CA	3
	3	Online Certification using Simple CMC: Certification of User Generated Single Key Pair by Participant CA	0
	4	Online Certification using Simple CMC: Certification of User Generated Single Key Pair by Reference CA	1
Test group 3 total			**4**
4	1	Validation: Reference Client, Reference Responder, Participant CRL	0
	2	Validation: Reference Client, Participant Responder, Reference CRL	2
	3	Validation: Reference Client, Participant Responder, Participant CRL	1
	4	Validation: Participant Client, Reference Responder, Reference CRL	1
Test group 4 total			**4**

Table 5: Executed tests

All the tests reported were successful.

If the number of executed tests are compared with the maximum number of tests possible in each test group, it can be seen that the tests related to inter-CA cross certification and subordinate were most popular with the participants.

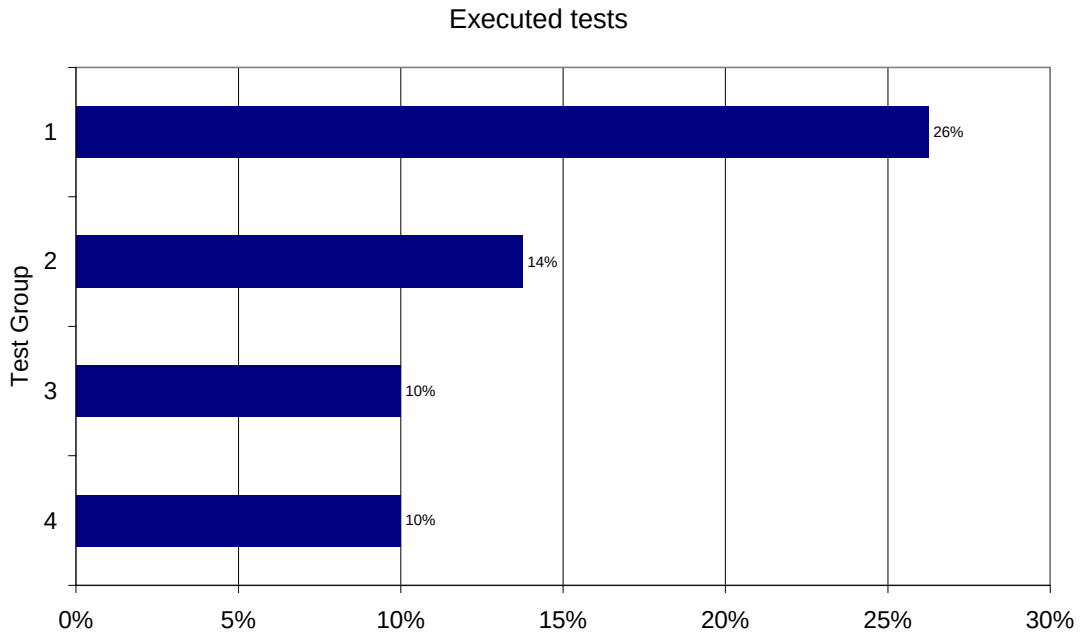

Figure 10: Executed Tests

3.4.2 Testing Participants

10 Testing Participants uploaded their test results. The following graph shows their participation in the total number of tests.

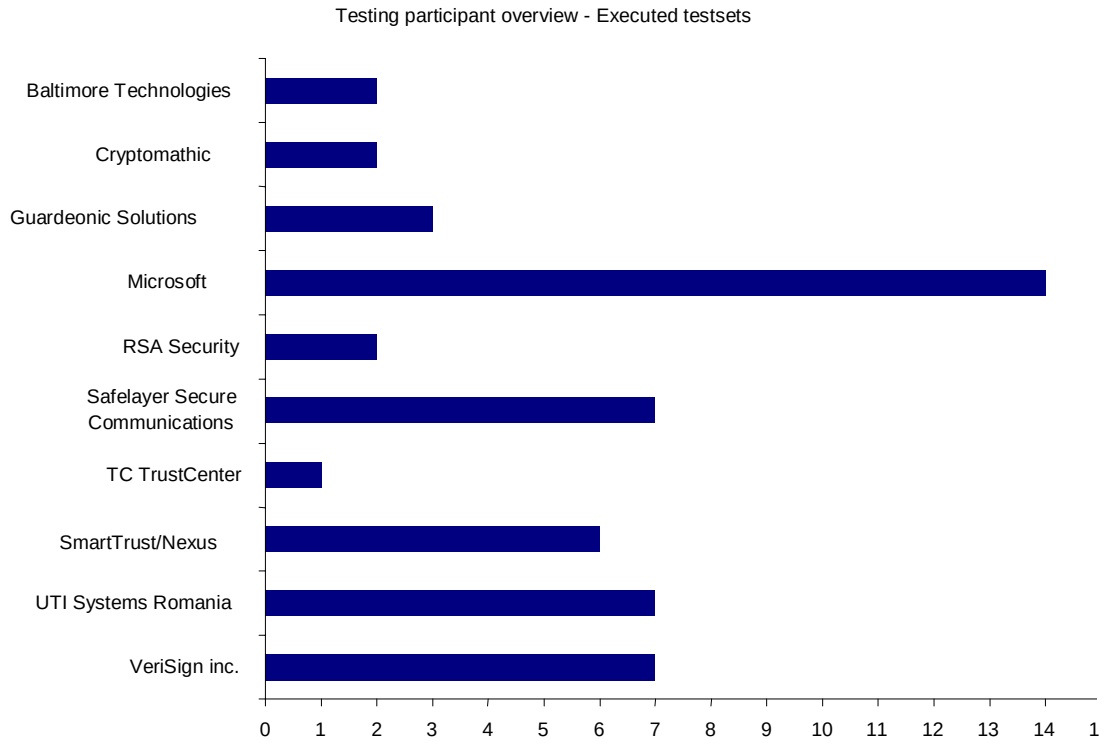

Figure 11: Testing Participant Overview

3.5 Non Technical problems

3.5.1 Priorities

The pressure that the prevailing economic climate placed on the Testing Participants to concentrate on revenue-earning business meant that most could only participate in the pkiC in bursts. It also meant that some could not participate at all. There were very few that could dedicate full-time resources to the process.

3.5.2 The MaxWare Virtual Directory (MVD)

The decision to use a Virtual Directory, coupled with the use of a published, agreed Directory structure was made to try to avoid the known problems with inconsistent Directory use. Despite widespread publicity, some of the Testing Participants were not aware that they were supposed to be using it. There was clearly a breakdown in communications with those Testing Participants and their progress was hampered by this lack of knowledge. All of the Testing Participants were represented at the Consortium meetings where the Virtual Directory issues were discussed and agreed, although those attendees were not necessarily the technical people involved in the testing.

4 Test results and recommendations

This chapter presents the major findings of the test process. These issues can be grouped into three blocks:

- Manual processes versus on-line processes
- Interoperability issues
- Other technical issues

4.1 Manual processes versus on-line processes

During the design stages for the pkiC there was considerable discussion regarding the transport mechanisms that should be supported. The relative merits of CMC and CMP were presented and it was decided that the test process support as many as possible. The Web site was built to support both CMP and Simple CMC. As a backup, it was also designed to support the manual processes in the event that the Testing Participants' systems did not support automatic processes. Nearly all of the Testing Participants chose to use the manual, backup mechanisms. This was not an expected outcome.

Conclusions

Automated processes were mostly relevant to end-entity enrolment and cross-certification. It seems likely that many products do not yet fully support automated processes, although the reduced testing period might also have caused the Testing Participants to prefer manual enrolment.

It was felt that the lack of support for automated cross-certification is not an issue for the industry. The mechanics of cross certification are the culmination of a legal process and are not performed often. Automated cross certification is unlikely to become the preferred method.

End-entity enrolment will be more of a problem for operational (rather than technical) interoperability if it remains a manual process. Any process that requires manual intervention creates unacceptably high costs. Automatic enrolment is only available by default in proprietary architectures, locking the customer into a specific PKI.

Recommendation

- The security industry should address the issue of automatic enrolment by supporting at least Simple CMC.

4.2 Interoperability issues

4.2.1 Subject Key Identifier (SKI) length

Subsequent to performing a cross-certification a Participant was experiencing a persistent failure in trying to prove the trust relationship through signed e-mail. Debugging revealed that the e-mail client was using SKI/AKI linking to construct the trust path and that the SKI computed by the Participant CA for its Root CA certificate and included in its PKCS#10 cross-certification request was different to the SKI value ***re-computed*** by the Reference System CA during the cross-certification process.

Further investigations revealed that the Participant CA had been configured to issue 60-bit Key Identifiers. This was in contravention of D2.2 which specified that 160-bit Key Identifiers should be used. The Reference System was thus re-computing the Participant SKI to 160-bits during the cross-certification process. The consequent AKI/SKI mismatch was the likely cause of the e-mail client's failure to construct a trust path.

The problem was mitigated by using DNs instead of Key Identifiers when constructing the trust path.

The problem was remedied by changing the Reference System so that instead of re-computing the SKI in the submitted PKCS#10 it ***copied*** the Participant's SKI from the PKCS#10 into the cross-certificate.

Recommendations

- PKI vendors should use 160-bit key lengths for Key Identifiers, although 60-bits should be supported for backward compatibility.
- Key Identifiers should only be computed where they do not already exist, as stated in RFC 2459/3280.

4.2.2 Subject Key Identifier (SKI) value

Subsequent to performing a cross-certification, a Participant was experiencing a persistent failure in trying to prove the trust relationship through signed e-mail. Debugging revealed that the e-mail client was using SKI/AKI linking to construct the trust path and that the SKI computed by the Participant CA for its Root CA certificate and included in its PKCS#10 cross-certification request was different to the SKI value ***re-computed*** by the Reference System CA during the cross-certification process.

Further investigations revealed that the Reference System was using an incorrect method[7] to generate the SKI value during the cross-certification process. The re-computed SKI inserted into the cross-certificate was different to that created by the Participant CA when generating the PKCS#10 request for cross-certification. The consequent AKI/SKI mismatch was the likely cause of the e-mail client's failure to construct a trust path.

The problem was mitigated by using DNs instead of Key Identifiers when constructing the trust path.

The problem was remedied by changing the Reference System so that instead of re-computing the SKI in the submitted PKCS#10 it ***copied*** the Participants SKI from the PKCS#10 into the certificate.

Recommendations

- When creating a SHA-1 Key Identifier, PKI products should calculate the value using the Public Key excluding the tag, the length, and the number of unused bits as per RFC 2459/3280.

4.2.3 Unsigned PKCS#10s

Enrolments from the Reference System to the Participant System (subordination of the CA) were achieved by way of pre-generated PKCS#10 request files that were posted to the Web

[7] The Reference System was using key value with tag, length and unused bits. The approved method is key value ***without*** tag, length and unused bits.

site. The Participant downloaded the PKCS#10 from the web site, processed it and uploaded the subsequent PKCS#7[8]. One of the Participants found that they could not perform this process because the CAs to which the requests pertained did not sign the PKCS #10s.

Although allowed (though not recommended) by the standards this was in contravention of the specifications contained in D2.2, which required that Proof of Possession of the private key be carried out.

The problem was remedied by replacing the unsigned PKCS#10s with signed PKCS#10s.

Recommendation

- Certification Request files (PKCS#10), for cross-certification or subordination, should always be signed by the CA, so that Proof of Possession of the CA's private signing key can be carried out.

4.2.4 AuthorityInformationAccess (AIA) encoding

During testing a Participant found that the EE certificates did not contain the AIA extension and that where it occurred in the CA certificates it was encoded incorrectly. This prevented the client software from performing an OCSP validation check on the certificate.

The problem was remedied by altering the reference system so that the AIA was correctly encoded and include in both EE certificates and CA certificates.

4.2.5 CRL Distribution Point (CDP) encoding

During testing a Participant found that the encoding for the CDP in CA certificates was incorrect and it was absent from EE certificates. This prevented the recovery of CRLs from the publisher's directory during certificate verification.

The problem was remedied by altering the reference system so that the CDP was correctly encoded and include in both EE certificates and CA certificates.

4.2.6 Components in the Distinguished Name (DN)

Many Participants implemented Directory schemas that did not match the specification contained in D2.2 (Interoperability Test Criteria). For the most part these discrepancies were ignored by the Reference System which responded to the request but did not publish the resultant certificate to the directory as there was nowhere in the supporting DIT[9] that would reflect the DN. In nearly all cases, this DIT non-conformance involved either extra or missing X.500 structural objects.

Conclusions

It is clear that the minimum set of attributes defined in D2.2 was not enough to accommodate the major PKI systems that were currently available. It is equally clear that some of those systems also have problems supporting that minimal list.

There were still a large number of interoperability problems caused by the structure and flexibility allowed in the Directory components, particularly, in this case, in the

[8] PKCS#7 is a PKCS#7 file – a file containing a public certificate
[9] DIT – Directory Information Tree, the structure of the Directory

Distinguished Name. The issue causes problems in the real world for both certificate and CRL retrieval and needs to be addressed. It is, however, a complex problem that has no obvious solution and will require a collaborative effort by the major players in the Security Industry.

Recommendations

- All PKI systems should support the following minimum set of components in the Distinguished Name (DN):
  - C (country)
  - L (locality)
  - O (organisation)
  - OU (organisational unit)
  - CN (common name)
  - DC (domain component)
- Any other components found in the DN should not cause a system failure.
- The issue of Directory structure and certificate retrieval needs to be addressed by the industry. The problem is further outlined in the document "pkiC - Challenges for the PKI Industry (D8.4)".

4.2.7 OCSP Signing Certificate

One of the Participants experienced some difficulties because the same CA that issued the Certificate whose status was being checked did not sign the OCSP signing certificate issued to the Reference System OCSP Server. The OCSP signing certificate was issued by the Reference System Root CA while the Certificate whose status was being sought was published by the Reference System Sub CA. Investigations showed that while the trust model used by the Reference System complied with the recommendations in RFC2560, it was not the most widely adopted method. The test team acknowledged this but a lack of time and resources drove the design decision and precluded remedial action for a specific participant.

Conclusions

RFC2560 describes three valid response models for OCSP. The OCSP response must be signed using a key that must be one of:

1) the same that signed the certificate being checked; i.e. the response is signed by the CA that issued the certificate in question
2) one issued to an OCSP responder in a certificate that has “OCSP-Signing” in the ExtendedKeyUsage extension. That certificate must be issued by the CA that issued the certificate in question
3) one that is valid within a local configuration of OCSP signing authority for the certificate in question

Model 3 is the one used by the pkiC Reference System, whereas model 2 is probably the most widely deployed / supported.

Recommendation

- For the sake of interoperability, model 2 is preferred, as it is the most widely used.

4.2.8 Encoding of basicConstraints in End Entity certificates

One of the Participants could not validate the End Entity certificates issued to it from the Reference System. Debugging by their technicians revealed a problem with the

basicConstraints extension in the certificate. The CA field in this extension was set to the value FALSE which is the default value for this attribute. The ASN.1 Distinguished Encoding Rules (DER) state that if an attribute has the default value then it should not be included in the encoded certificate (Note that the ASN.1 Basic Encoding Rules (BER) **do** allow default values to be present.) The test team acknowledged this and the Reference System was altered to exclude the CA attribute from the basicConstraints extension in EE certificates and the tests proceeded successfully.

Further investigations, however, revealed that best practice recommends the inclusion of the basicConstraints CA field in EE certificates but that the field should have no value. This is to mitigate the risks of a rare spoofing condition present in the Microsoft Crypto-API for which there is now a patch available.

Conclusions

For the sake of interoperability, therefore, basicConstraints in EE with CA=NULL should be preferred.

This issue is an example of the complexity of the standards and how rules can be different even in different parts of the same standard (in this case between BER and DER of X.690).

Recommendations

- A PKI should encode basicConstraints in an End Entity certificate with the CA field set to no value (i.e. NULL)

4.3 Other Technical problems

4.3.1 Access to the pkiC interoperability Web site through the Royal Mail firewall

For the most part the requirement for the Testing Participants to provide the test team at Royal Mail with a non-DHCP address for the machine from where access would be required presented no significant issues. With only minor problems all the Testing Participants gained access to the Web site within 24 hours of submitting their IP addresses to the test team. There were two exceptions to this.

Conclusions

No major issues were found in the area of firewall access, except for one Testing Participant who appeared to be experiencing difficulties with their ISP. Rather than open up their own firewall or assign static IP addresses, some Participants chose to install their system in the Royal Mail laboratory.

Recommendation

- Information on firewall requirements, including specific port numbers, should be readily available to PKI users. This information is included in the Best Practice paper "pkiC – Best practice for PKI Users" (D8.2)

Port Number	Service	**Use**
(Definitely)		
829	PKIX	CA/RA communication
389	LDAP	Enquiring on-line LDAP directories
(Desirable)		
636	LDAP/S	SSL-enabled version of the above
80	HTTP	For recovering (e.g.) CRLs from a public location
443	HTTP/S	SSL enabled version of the above
143	IMAP	Mail transport for CMC communication
220	IMAP-3	Mail transport for CMC communication
585	IMAP/S	SSL enabled version of the above

Table 6: Specific Port Numbers

4.3.2 Mail system for CMC submission

A first attempt from one of the Participants to perform a Simple CMC-based Subordinate certificate received no reply from the Reference System. After some investigation it transpired that this was caused by the configuration in the firewall for the handling of IMAP requests. The firewall was reconfigured to process IMAP requests correctly within 24 hours of reporting the fault.

4.3.3 Re-certification of CAs and regeneration of download PKCS#10s

Following the detection and fix of many of the bugs in the Reference System it was often necessary to reissue the Root certificates and the Reference System PKCS#10s. This meant that, in many cases, the tests had to be repeated using the new certificates. There were inevitable delays.

Conclusions

The selection and configuration of the profiles and protocols used by a CA is critical; rebuilding and re-certifying a CA to correct a problem costs both time and money. Reissuing certificates to an entire community could be prohibitively expensive and could undermine an organisation's entire PKI strategy.

4.3.4 e-Mail clients

The fact that different e-mail clients worked in different ways presented huge problems when it came to the proof-of-trust stage in the test process. e-Mail client non-interoperability presented itself in a variety of different ways;

- Opaque signing versus Clear signing
- Certificate inclusion/exclusion
- Trust chain inclusion/exclusion
- Local storage versus LDAP lookup
- DIT/X.500 structure knowledge/presumptions
- Trust path construction
- Attachment Handling
- S/MIME v2/v3

Conclusions

It was not the purpose of the project to prove the compliance or otherwise of e-mail clients with the S/MIME standard but the differences between the clients meant that an exchange of signed e-mail to prove that a trust relationship had been established was not as straight-forward as envisaged. In retrospect it was perhaps a little naïve to assume that proof of trust could be established in all test cases. It was also a little shortsighted because proof of trust was only really relevant to those participants who actually had client software that they wanted to test. Requiring this from CA software providers was built on the false assumption that all e-mail clients would work correctly and behave in the same manner.

With regard to the e-mail clients used, the following observations can be made:-

S/MIME awareness

Not all e-mail clients are S/MIME-aware – a primary requirement for creating S/MIME messages.

S/MIME version

The most commonly deployed version of S/MIME is currently version 2. The version 3 standard has now been adopted so new deployments of e-mail clients should support version 3 as well as version 2 (for backward compatibility).

Enrolment

To support enrolment to any CA, e-mail clients must be capable of producing a PKCS#10, certification request file.

Creating trust paths

To create a trust path to a trusted root, an e-mail client requires access to all of the certificates in the trust chain. Ideally an e-mail client should be able to access a Directory to obtain the required certificates. However, not all e-mail clients support directory look-ups and all LDAP directory servers do not support searching for certificates. One way to mitigate this problem would be for e-mail clients to include the entire public certificate trust chain in outgoing e-mails for the EE certificate being used to create the signature. The receiving e-mail client then at least has the choice of accepting the offered trust it contains rather than not having access to any trust paths at all.

Revocation Checking

All e-mail clients should be capable of retrieving and processing CRLs, either Partitioned or Consolidated. They should also ideally support OCSP.

Managing the trust store

Having access to the certificate store(s) on the e-mail client, for example to install trusted root certificates helped to solve some problems during testing. This is not always desirable for end users and depends on company security policy. See the Best Practice paper “pkiC – Best practice for PKI Users” (D8.2) for more discussion on this topic.

4.3.5 Non-compliance with test specification

As mentioned earlier, the completion and agreement of D2.2 was compromised by the withdrawal from the project at a critical time by Entegrity whose task it was to write the document. Even so, it was generally accepted that in spite of some disputed content, D2.2

was the standard to which the Testing Participants should subscribe. Unfortunately compliance to D2.2 by the Testing Participants was not always achieved and this led to problems and delays in testing that could otherwise have been avoided. The two areas of non-compliance detected were;

- The structure of the Participant's supporting directory
- Key identity lengths (e.g. AKI/SKI)

4.3.6 Royal Mail Web site specific issues

There were problems with the usability of the pkiC interoperability Web site with respect to the submission of PKCS#10s by the Testing Participants. The database that supported the CAs in the Reference System was very sensitive to the reuse of information in the PKCS#10s. In particular it rejected any attempt to reuse either already submitted keys or already published Distinguished Names. It was also critical that the Testing Participant specify the correct format for the PKCS#10 file at upload so that the CA would know how to process it. This last point was merely a learning curve issue but the former two points caused repeated problems. The lack of error reporting from the CAs to the web site made problem resolution of this nature somewhat laborious.

Conclusions

The attempted reuse of Distinguished Names (DN) was probably exacerbated by the artificial environment created by the project and should be less of a problem in practice. Most Certification Authorities will ensure that a DN is always unique by including the certificate serial number as one of the components (and this is bad practice from a directory perspective).

The reuse of public keys is not strictly an interoperability issue but it could cause problems, depending on the circumstances. It is, however, bad practice and should be avoided.

Recommendation

- Public keys should not be reused

4.4 Best practices

All the conclusions and recommendations are used as the basis for three other documents produced as an extension to the project. The intention of these documents is to provide clear "Best Practice" PKI guidelines for different interest groups: vendors, users and industry.

5 Impact of the pkiC

5.1 Comparison with the project objectives and evaluation criteria

Summarised, the two main objectives within the pkiC were:

- Creating a framework for PKI security products and PKI service providers to prove the possibility of working together, based on international established standards.
- Promotion of practical solutions for Secure Electronic Commerce integration across Europe

The first objective was fulfilled by the successful implementation of the reference system and the number of tests positively completed by the different participants.

Although not all the milestones were met for giving demonstrations, it is possible to say that also the second objective was fulfilled successfully, based on the press coverage and the general interest within and without Europe (see annexes C and D).

5.2 Relation with other relevant projects

5.2.1 Co-operation with UK Government CESG initiatives

The pkiC project had its initial Project Board meeting on 31st January 2001 after a gestation period of 18 months. The initiative for the project came from the industry membership of EEMA with encouragement from the Commission of the European Union. It was perceived that the lack of the general availability of interoperable PKI products and services constituted a barrier to the successful deployment of e-Commerce solutions across Europe and, indeed, across the world.

Meanwhile, and quite independently within UK Central Government, e-Government initiatives were being put in place with a target date of end fiscal year 2005 to have 100% of relevant Government services accessible on-line. Again, the lack of generally available interoperable PKI products and services was perceived to be holding back these initiatives. The driver for the e-Government initiatives is the Office of the e-Envoy. This is part of the Cabinet Office. One of the key policy documents published by the Office of the e-Envoy is entitled "The e-Government Interoperability Framework" otherwise known as e-GIF. To quote from this, the UK Government Policy for e-mail is:

"To use a product that supports interfaces which conform to the SMTP/MIME. Within government, the norm will be to use the intrinsic security provided by the GSI to ensure e-mail confidentiality. Outside GSI and other secure government networks, S/MIME V3 should be used for secure messaging".

In recognition of this situation, the Office of the e-Envoy funded CESG to conduct interoperability tests in order to encourage the PKI vendor and services community to move towards the provision of PKI products and services that were interoperable. The focus of these tests was secure e-mail interoperability.

The management of pkiC became aware of the CESG activity in early February 2001 and the Project Manager made contact with the Office of the e-Envoy with a view to exploring the possibilities of collaboration with CESG. The upshot of this was an invitation by CESG to

pkiC to make a short presentation on pkiC at the CESG event in Ashford. This Open Day was used to present the results of the first tranche of interoperability testing conducted by CESG in Cheltenham. After subsequent correspondence between pkiC and CESG, a meeting was arranged at CESG in Cheltenham on 27th April 2001. Subsequently, the two projects entered a period of collaboration where presentations were made at each other's meetings and test specifications were exchanged to ensure a degree of harmonisation was in place. A second and final tranche of interoperability testing took place early in 2002 at Cheltenham. Thereafter, the Office of the e-Envoy referred to the activities of pkiC within UK Government departmental circles as taking forward the interoperability initiatives of the CESG. Many of the pkiC Testing Participants also took part in the CESG tests and the information gleaned in the CESG tests were carried forward into the pkiC tests.

5.2.2 Cooperation with the PKI Forum

In the early stages of the pkiC project, a liaison agreement was closed with the PKI Forum, a worldwide initiative dealing with interoperability topics in different PKI areas. The cooperation was especially successful in the area of information exchange by presenting the pkiC in the PKI Forum meetings and by presenting the results to each other if applicable.

5.3 Implications on standards and EU policies

One of the implications from this interoperability-testing project is that the existing standards are far too complex, and have far too many options, to ensure that different vendors can build fully interoperable systems from them. Profiling the standards would seem to be essential. But even then, this may not be enough. Specification D2.2 was a simple profile of the PKI related standards, but even this proved to be too complex for any of the vendors fully to test against e.g. no CMP testing was done at all. Given that the EESSI specifications add yet another layer of complexity to the existing international standards, one must question if these specifications will ever be implemented in their entirety, if at all. It would appear that currently the cost is too great, and the market is too small to make this economically feasible. The implication for the EU is that fewer and simpler, rather than more and complex, standards are needed.

The EU should consider a policy of more stringent profiling, with a much greater level of detail than is currently employed e.g. specifying exactly the bits that should be contained in fields such as the subject key identifier, rather than simply saying that a field should be present. In a similar vein, the problems that are experienced with directory services, would indicate that more stringent requirements should be placed on directory names and DIT structures, rather than allowing the current "anything goes" policy, which this report indicates is a major cause of interoperability problems.

The tests carried out by pkiC identified a number of areas where the existing specifications could be improved. These can be brought to the attention of those in the standards community by promulgating the results of this project.

However, this process of testing implementations and refining the standard specifications to produce interoperable implementations should be more of an integral part of the standardisation process. The support of trials such as pkiC early in the development process of standards would greatly improve the quality of the resulting standards and greatly improve the chances of suppliers developing products that are truly interoperable. Thus, it is suggested that the importance of trials such as pkiC is brought to the attention of EU policy

makers and that suppliers be encouraged to participate in such trials as early as possible in the standardisation process.

5.4 Project benefits

The approach taken by the pkiC to use a central reference system has proven to be successful. The fact that nearly all the participants were competitors of each other had no impact on testing against the reference system. It is proven in the pkiC that PKI technology can work against a standard reference system from a technical perspective, but it takes a lot of hard work, effort and money. Pair wise interworking unfortunately could not be proven in this project due to lack of time and resources.

That testing against the Reference Implementation was successful is even more remarkable bearing in mind the difficult economic situation of the last two years. Nearly every participant was limited in resources to work on the project, but even then they were able to achieve interoperability on the most important test areas.

The pkiC must give governments and the industry more confidence in the PKI technology as such. However, it is appreciated that it does not yet give full confidence due to the limited number of tests that were completed successfully. Never the less, the situation improved during the life of the project, and it can be expected to continue to improve. Installing a PKI from a certain vendor does not mean that an organisation has an isolated solution without any interoperability possibilities, but some best practice rules regarding the settings on the CA and the certificate have to be kept in mind (see the “Best Practice” documents). Another major problem for a break-through of PKI technology is not the CA technology itself, but more the PKI related technologies, such as the issues with S/MIME clients and LDAP/X.500 directories (but note that a current development within the IETF PKIX group[10] and OpenLDAP implementation will soon allow PKI clients to search for public key certificates and CRLs in LDAP directories).

[10] Klasen, N., Gietz, P. "An LDAPv3 Schema for X.509 Certificates", <draft-klasen-ldap-x509certificate-schema-02.txt>, March, 2003
Chadwick, D.W., Sahalayev, M. V. "Internet X.509 Public Key Infrastructure LDAP Schema for X.509 CRLs", <draft-ietf-pkix-ldap-crl-schema-00.txt>, February 2003
Chadwick, D.W., Sahalayev, M. V. "Internet X.509 Public Key Infrastructure LDAP Schema for X.509 Attribute Certificates, <draft-ietf-pkix-ldap-ac-schema-00.txt>, February 2003

6 Outlook

6.1 Future of the current reference system

With the agreement of the European Commission, Utimaco Safeware AG decided to adopt the pkiC reference system to allow their partners and customers to test against it.

6.2 Standardisation

The possibility for placing the pkiC recommendations as defined in chapter 0 in the standardisation domain will be examined by EEMA.

6.3 Potential new projects derived from the pkiC

Directly related to the outcome from this project, the following potential new potential testing areas can be derived:

- Continuing the work started in the pkiC with a better focus on on-line CMP testing
- Extending the pkiC with time stamping
- Instead of continuing with a reference system for interoperability testing, create a kind of "PKI vendor switching board", hosted by an independent company to allow Pair wise testing between vendors on request.
- Use the experiences gathered during the interoperability tests within the concept of the European Bridge CA.

The pkiC has also shown a few interoperability issues in related technologies. This means that also in that area some work should be done:

- Interoperability between S/MIME clients (e-mail clients)
- X.500 directory interoperability
- Smart card – PKI and smart card – PKA[11] interoperability testing (within the scope of the eEurope Smart Card Charter)
- Technology investigation to create a PKI environment within the scope of the EU directive

Some of these areas are already under investigation in other interoperability initiatives e.g. S/MIME in CESG and in Sphinx and CMP testing in the PKI Forum. In a short questionnaire launched at the end of the pkiC project towards the testing participants, a clear preference was shown for a project dealing with all the requirements needed for PKI solutions within the framework of the EU directive and the EU-members legislation.
An other general interest of the participants is the creation of a PKI vendor switching board to get a better view on the interoperability aspects in pair wise testing instead of working with a reference system.

6.4 Sixth Framework Programme (FP6)

The Sixth Framework Programme for Research and Technological Development (FP6) is a decisive step towards marshalling Europe's research and scientific networks and the European Union into the most dynamic and competitive knowledge-based economy in the world.

[11] PKA: PKI enabled Applications

FP6 is the Union's main instrument for funding research in Europe Proposed by the European Commission and adopted on 3 June 2002 by the Council of Ministers and European Parliament, it is open to public and private entities, large or small, for four years from the end of 2002 through to 2006.

The overall budget for FP6 is 17.5 billion Euro, representing 3.4 % of the EU's total budget in 2002.

Within this total, 12 billion Euro has been set aside for seven key areas or 'thematic priorities' earmarked to achieve FP6 objectives. One of these key areas is 'Information Society Technologies' (3.625 billion Euro).

Within this key area, several opportunities for security projects arise in a larger context of the 'all digital world'. There are two major objectives identified where security could play a leading role: protecting the rights and the privacy of the citizens and secure transaction by means of electronic and mobile commerce.

7 Conclusions & recommendations

Although the difficulties faced during the project related to the consortium and the reference system, it is possible to state that the project was successful in achieving basic PKI interoperability. The most important conclusion that can be taken is the fact that cross certification between different CAs (root CA or sub CA) is possible using a manual process without problems. Nevertheless, a few guidelines have to be kept in mind when an organisation wants to initiate such a process as a PKI customer or a PKI Service provider.

On the other hand, a clear recommendation for the future is widespread adoption of the automatic protocols to achieve PKI interoperability, such as Simple CMC and CMP. Besides the PKI interoperability itself, the pkiC has also identified other technical problems that could slow down the acceptance process of the technology. Another recommendation for the future is to examine S/MIME interoperability and the connection between PKI and Directory systems.

The organisational difficulties faced during the first part of the project caused some delays in the preparation of the tests. The result was that some of the participants had insufficient time to test their products during the testing phase. A future project should foresee more time for the real testing phase so that the testing participants have more freedom to set their priorities both to their on-going projects **and** to the interoperability project.

The technical recommendations made in chapter 4 should be presented to the standardisation bodies to improve interoperability. In general, the importance of trials such as the PkiC should be encouraged as early as possible in the standardisation process to validate the quality of standards being tested and encourage interoperable implementations.

From the marketing perspective, which was a secondary objective of the project, the project was successful as well. The goal, the approach and the results of the pkiC were published in several specialised magazines and were presented at major European security conferences.

Based on the enthusiasm and the number of testing participants, it makes sense to think about a new derived security project for the future, especially if it can be linked to the new EU Sixth Framework Programme. The testing participants are especially interested in a new project to check their product against the EU directive on a Community Framework for electronic signatures (1999/93/EC) and the national implementations of this directive.

Annex A: Testing Participants

This annex will give a short overview of all the tests executed by each Testing Participant. To get more information about the tests and the products used to perform the tests please see Annex B for the correct with a point of contact

Besides the testing participants the following companies showed their interest in the pkiC, but in the end did not perform any of the tests for several reasons: Ascertia, Entrust, NetSet, SSH and Valicert.

The tests that were conducted by participants covered the following interfaces:

- Basic S/MIME Client Interoperability
- TG1 - Mutual Root Cross Certification
- TG2 – Subordinate CA Certification
- TG3 – Enrolment
- TG4 – Certificate Validation

Of these tests, S/MIME Client Interoperability is not reported herein, but was a required precursor to any tests involving the exchange of signed and encrypted messages. The results of following Testing Participants are described.

Baltimore

CRYPTOMAThIC

Guardeonic Solutions

Microsoft

RSA Security

Safelayer Secure Communications

SmartTrust/Nexus

TC TrustCenter

UTI Systems Romania

Verisign/BTIgnite

A.1 Baltimore Technologies

A.1.1 Test Setup

Conducted online testing from their facility in Ireland. The summary results described herein are derived from the document, which they submitted at the end of testing.

The product tested was Baltimore Unicert version 5.0.1.2.
The CA repository was IPlanet 5.1.
The e-mail client used to conduct the tests was Outlook 2000 with Securenet Mailsecure 4.
No validation authority was configured.

Baltimore created a pki environment with a root, and subordinate CA (root cn = DEMO_CA, sub cn = BALTIMORE_CA).

A.1.2 Tests

A.1.2.1 Test Group 1 – Cross Certification

Baltimore conducted the following tests in this group:

- Participant Root CA certifies Reference Root CA
- Reference Root CA certifies Participant Root CA

Baltimore successfully conducted Mutual Cross-Certification, and Mutual Trust between the Baltimore Root CA and the Reference Root CA in TG 1. The Manual Unidirectional Cross-Certifications in both directions were performed as steps to complete the Mutual Cross-Certification test.

Conclusion

Baltimore appears to have successfully completed Mutual Cross-Certification between Root CAs.

A.1.2.2 Test Group 2 – Subordinate CA Certification

Baltimore conducted the following tests in this group:

- Reference Root CA certifies Participant Subordinate CA
- Participant Root CA certifies Reference Subordinate CA

Conclusion

Baltimore successfully completed the core tests in this test group.

A.1.2.3 Test Group 3 – Enrolment

Baltimore ran a number of tests relating to enrolment using a secure e-mail plug-in, Mailsecure, from Securenet Australia. Enrolment was not a formal part of the Baltimore test suite, but there were, nonetheless, interesting preliminary test results.

A.1.2.4 Test Group 4 – Certificate Validation and Path Construction

Baltimore was successful in validating the status of the test users while at the same time encountering issues with both the directory and CRL handling of the plug in chosen. As such, these tests were also preliminary, but the results were interesting given that the only problems encountered were minor and did allow for a proof of concept exercise at the client level.

A.2 CRYPTOMAThIC

A.2.1 Test Setup

Cryptomathic conducted online testing from their facility in Cambridge, England. The summary results described herein are derived from the document, which they submitted at the end of testing.

The product tested was Cryptomathic Certificate Authority CCA version 3.3.1.156.
Sun IPlanet Directory server was used as the certificate repository.
Microsoft Outlook Express was the e-mail client used to conduct the tests.
An OCSP Responder was not configured.

The Cryptomathic Certification Authority client application was used to create a PKI environment with a root, subordinate, and sub-subordinate CAs (uids = crmroot, crmsub, crmsubsub and o = crm).

After each of the CAs had been created Cryptomathic created the chain between all three CAs.

Cryptomathic used an LDAP tool to manually publish the certificates to the directory.

A.2.2 Tests

It was the original aim of Cryptomathic to complete three of the four test groups, cross certification, subordinate CA certification and enrolment. Test group one was completed successfully but due to features of our CA system conflicting with the requirements of the Reference Implementation (described below) the second and third tests could not be completed as specified by the test specification.

A.2.2.1 Test Group 1 – Cross Certification

Cryptomathic successfully conducted the following tests in this subgroup:

- Participant Root CA certifies Reference Root CA
- Reference Root CA certifies Participant Root CA

Cryptomathic conducted the Manual Mutual Cross-Certification, and Mutual Trust between the Participant Root CA to the Reference Root CA in TG 1. The Manual Unidirectional Cross-Certifications in both directions were performed as steps to complete the Mutual Cross-Certification test.

Cryptomathic also attempted the Secure e-Mail Basic PKI Environment Interoperability Test for Root CA Mutual Cross Certification in this test group (TG1 – Test 3), however these tests could not be completed because of errors in the Reference Implementation.

Conclusion

Cryptomathic successfully performed Mutual Cross-Certification between the Cryptomathic Root CA and the Reference Root CA.

A.2.2.2 Test Group 2 – Subordinate CA Certification

The second test, which we initially intended doing, could not be completed due to the fact that our system is composed of C.A.s which must initially construct self signed certificates. Each C.A. is thereby initially set up as an autonomous C.A. before they can become part of a hierarchy. This is in keeping with the way the majority of systems in use today operate. Despite this, the reference system chose to implement a different system, where the subordinate C.A.s and the sub-subordinate C.A.s only exist as dependents on/subordinate of the root C.A. and should anything happen to the root C.A. or should its keys be compromised, all C.A.s in the chain/PKI are made obsolete. Because of this, our system required self signed certificate requests (PKCS#10s), rather than the certificate requests signed by the root C.A., sent from the pkiC subordinate C.A. as mandated by the reference system. This difference in design between the reference C.A. and our more traditional C.A. meant that the process could not be completed.

Conclusion

Cryptomathic did not perform any of the tests in this test group due to the Reference Implementation not being able to provide self-signed certificate requests.

A.2.2.3 Test Group 3 – Enrolment

The third test involved taking a certificate request from the reference system such that a certificate could be issued for a reference end entity and visa versa, in that it was requested that our system send a certificate request to the reference system such that they could issue a certificate for our end entity. Unfortunately our system does not allow for the end entity to create their own certificate requests nor does it allow for the Web-based enrolment system to take a certificate request and issue a certificate via this application.
All generation of PKCS#10s goes on behind the scenes and is managed by the client software, in this case Microsoft, and cannot be extracted nor input into the system. The reason for this is to ensure a smooth user registration, rather than requiring user intervention.

Conclusion

Cryptomathic did not perform any of the tests in this test group

A.2.2.4 Test Group 4 – Certificate Validation and Path Construction

Conclusion

Cryptomathic never intended to perform nor did not perform any of the tests in this test group since these tests are more suited to client-side components rather than the C.A. component under test.

A.3 Guardeonic Solutions

A.3.1 Test Setup

The product tested was **TrustedCA**.
TrustedMIME was the e-mail client used to conduct the tests.
A directory server / repository was not configured due to time constraints and network configuration problems on the Guardeonic Solutions side.
An OCSP Responder was not configured.
Guardeonic Solutions configured a PKI environment consisting of a three-tier hierarchy (RootCA, SubCA and Sub-SubCA) in accordance with the reference system a single Root CA.

A.3.2 Tests

A.3.2.1 Test Group 1 – Cross Certification

Guardeonic Solutions conducted the following tests within this group:

- Participant Root CA Cross Certifies Reference Root CA
- Reference Root CA certifies Participant Root CA

Conclusion

Guardeonic Solutions' TrustedCA demonstrated the capability to handle cross-certification in both directions.
As Guardeonic Solutions were not in the position to configure an LDAP directory, certificate publishing was not tested; nor could the simple SMIME trust tests before and after cross certification be performed because of problems with the reference system handling of Key Identifiers.

A.3.2.2 Test Group 2 – Subordinate CA Certification

Guardeonic Solutions conducted the following tests in this group:

- Participant Root CA certifies Reference Subordinate CA
- Participant Root CA certifies Reference Sub Subordinate CA (this test was not part of the test plan, but was completed by the Participant)

Conclusion

Guardeonic Solutions successfully performed the core Subordinate CA Certification tests.

A.3.2.3 Test Group 3 – Enrolment

Conclusion

Due to time constraints, Guardeonic Solutions did not perform any of the tests in this test group

A.3.2.4 Test Group 4 – Certificate Validation and Path Construction

Conclusion

Due to time constraints Guardeonic Solutions did not perform any of the tests in this test group

A.4 Microsoft

A.4.1 Test Setup

Microsoft conducted tests at the testing facility in Chesterfield. The summary results described herein are derived from the document, which they submitted at the end of testing.

The CA product tested was Microsoft Windows 2003 Enterprise Server (RC1) Certificate Services.
The repository used was Microsoft Windows 2003 Enterprise Server (RC1) Active Directory.
The Client product tested was Microsoft Outlook Express 6.
The OCSP responder used was the Alacris OCSP Server v1.1.

A.4.2 Tests

Microsoft conducted the most tests of any participant, and also produced the most detailed test reports. The tests conducted covered the following interfaces:

TG1 – Mutual Root Cross Certification (Manual and via CMC)
TG2 – Subordinate CA Certification
TG3 – Enrolment
TG4 – Validation

A.4.2.1 Test Group 1 – Cross Certification

TG1 Test 1.1 – Manual and Simple CMC one-way trust

The Manual Unidirectional Cross-Certifications in both directions (tests 1.1.1 and 1.1.2) were performed as steps to complete the Mutual Cross-Certification test (test 1.1.3).

These tests were also done using CMC. Note that although a CMC enrolment was performed, the individual tests (revocation, expiration, etc.) were not carried out since the CMC enrolment produced an identical certificate to the manual enrolment process.

TG1 Test 2 - Advanced Test – Root CA Cross Certification - Most of the Advanced Tests for Root CA Cross Certification were covered in either test 1.1, test 3 or in the Validation test group (for OCSP revocation checking). Microsoft did not attempt the policy check test.

TG1 Test 3 – Interoperability Scenarios:- Secure e-Mail Basic PKI Environment – This test was completed.

Conclusion

Microsoft successfully performed Manual Cross-Certification between the Microsoft Root CA and the Reference Root CA manually and using CMC. Microsoft also successfully conducted the TG1 Mutual Root Cross-certification Interoperability Scenario: - Secure e-Mail Basic PKI Environment.

A.4.2.2 Test Group 2 – Subordinate CA Certification

Microsoft performed all of the tests in this group in so far as it was possible, they are summarised as follows:

- TEST 1. BASIC TEST – SUBORDINATE CA CERTIFICATION
  - Test 1.1.1 - Participant Root CA certifies Reference Subordinate CA
  - Test 1.1.2 - Reference Root CA certifies Participant Subordinate CA
  - Test 1.1.3 - Participant Subordinate CA certifies Reference Sub-Subordinate CA
  - Test 1.1.4 - Reference Subordinate CA certifies Participant Sub-Subordinate CA (dep)
- Test 1.2 – AUTOMATED SUBORDINATE CA CERTIFICATION USING SIMPLE CMC
  - Test 1.2.1 – Participant Root CA certifies Reference Subordinate CA
  - Test 1.2.2 – Reference Root CA certifies Participant Subordinate CA
  - Test 1.2.3 – Participant Subordinate CA certifies Reference Sub-Subordinate CA
- Test 3 - SECURE EMAIL INTEROPERABILITY TESTS FOR SUBORDINATE CA CERTIFICATION
  - SECURE EMAIL INTEROPERABILITY TESTS (ROOT CA CERTIFIED SUBORDINATE CA)
    - Test 3.1 – Participant Root CA certified Reference Subordinate CA
    - Test 3.2 – Reference Root CA certified Participant Subordinate CA
  - SECURE EMAIL INTEROPERABILITY TESTS (SUBORDINATE CA CERTIFIED SUB-SUBORDINATE CA)
    - Test 3.3 – Participant Subordinate CA certified Reference Sub-Subordinate CA
    - Test 3.4 – Reference Subordinate CA certified Participant Sub-Subordinate CA (deprecated)

Conclusion

Microsoft successfully performed the TG2 Sub-Certification tests via the manual method and using Simple CMC. Microsoft also successfully conducted the TG2 Sub-certification Interoperability Scenarios using the Secure e-Mail Basic PKI Environment.

A.4.2.3 Test Group 3 – Enrolment

Microsoft conducted the following tests in this group:

- ONLINE ENROLMENT
  - Test 3.1.1.1 – On-line Enrolment using Participant Client-side key generation
  - Test 3.1.1.2 – On-line Enrolment using Reference Client-side key generation
- MANUAL ENROLMENT
  - Test 3.2.1.1 – Manual Enrolment using Participant Client-side key generation
  - Test 3.2.1.2 – Manual Enrolment using Reference Client-side key generation

Conclusion

Microsoft successfully performed the core tests in TG 3 Enrolment.

A.4.2.4 Test Group 4 – Certificate Validation and Path Construction

Microsoft conducted the following tests in this group:

- PARTICIPANT CLIENT, PARTICIPANT RESPONDER, PARTICIPANT CRL
  - TG5.1.1 configured with a valid crl
  - TG5.1.2 configured with an expired crl
- REFERENCE CLIENT, PARTICIPANT RESPONDER, PARTICIPANT CRL
  - TG5.2.1 Configured With A Valid CRL
  - TG5.2.2 Configured With An Expired CRL
- PARTICIPANT CLIENT, PARTICIPANT RESPONDER, REFERENCE CRL
  - TG5.3.1 Configured With A Valid CRL
  - TG5.3.2 Configured With An Expired CRL
- REFERENCE CLIENT, PARTICIPANT RESPONDER, REFERENCE CRL
  - TG5.4.1 Configured With A Valid CRL
- REFERENCE CLIENT, PARTICIPANT RESPONDER, REFERENCE CRL
  - TG5.4.1 Configured With A Valid CRL

Conclusion

Microsoft successfully performed the core tests in TG4 Validation.

A.5 RSA Security

A.5.1 Test Setup

RSA Security could not participate in the online testing, due to Corporate Network Security policies, and decided to perform the testing in the lab of Royal Mail in Chesterfield.

The product RSA tested was RSA Keon CA version 6.02, in association with a Sun ONE Directory Server.
[Note: At the time of the testing, November 2002, the RSA Keon CA version 6.02 has been on the market since Spring 2002, and is now replaced with version 6.5, a Common Criteria EAL 4+ validated product]

The RSA Keon CA was configured with three Virtual CA's ("Root CA", "Sub CA", and "Sub Sub CA") were created and chained to create a required signing hierarchy.

The RSA Keon CA was configured to publish any issued certificates and CRLs to a Sun ONE Directory Server, installed as the directory of choice in RSA's test environment. The MAXware Virtual Directory was set-up to access this directory server.

A.5.2 Tests

Based on a number of published documents from the pkiC, such as WP2 D2.2 and WP4 D4.3.0-4.3.4.

A.5.2.1 Test Group 1 – Cross Certification

RSA Security conducted the following tests:

TEST 1 BASIC TEST - ROOT CA CROSS-CERTIFICATION
- Manual Method: Reference Root CA Certifies Participant Root CA
- Manual Method: Participant Root CA Cross Certifies Reference Root CA

The Manual Unidirectional Cross-Certifications in both directions were performed as steps to complete the Mutual Cross-Certification test.

Conclusion

RSA Security successfully performed Manual Mutual Cross-Certification between the RSA Root CA to the Reference Root CA, and reported successful publication of the correct cross-certificate pairs (both with "IssuedToThisCA"/"Forward" and "IssuedByThisCA"/"Reverse" certificate) in the RSA installed directory, Sun ONE Directory Server.

A.5.2.2 Test Group 2 – Subordinate CA Certification

RSA Security originally intended to participate in the first four tests (1.1.1, 1.1.2, 1.1.3, and 1.1.4), but for reasons such as time limitation, and other, it was decided to not conduct these tests.

However, as part of the RSA Secured Partner programme, RSA has certified such interoperability with some CA-products available on the market.

Conclusion

RSA did not perform any of the tests in this test group

A.5.2.3Test Group 3 – Enrolment

RSA Security did not submit any client application, and the functionality of RSA Keon CA is not relying on any proprietary client software. However, RSA Security originally intended to participate in some tests of this group, using the Reference Client enrolling for certificate from the RSA Keon CA. For reasons such as time limitation, and other, it was decided to not conduct these tests.

Conclusion

RSA did not perform any of the tests in this test group

A.5.2.4 Test Group 4 – Certificate Validation and Path Construction

RSA Security did not submit any client application, and the functionality of RSA Keon CA is not relying on any proprietary client software. The test scenarios were based on two models, End-Entity client model and VA (Validation Authority) client/server model, and RSA Security did not participate in any tests of this group.

Conclusion

RSA did not perform any of the tests in this test group

A.6 Safelayer Secure Communications

Safelayer develops a whole set of solutions to safeguard all communications and commercial transactions conducted over networks between two entities (enterprises, the Public Sector and other entities) with their clients and users, thus building trusted relationship on a virtual environment.

Safelayer´s KeyOne® products for Digital Certification, Secure Validation, Time Stamping, Digital Signature and Data Encipherment are globally recognised solutions for their flexibility, scalability, interoperability and the ease with which they can be integrated both vertically in any sector and horizontally within any department of an organisation.

A.6.1 Test Setup

Safelayer conducted online testing from their facility in Barcelona. The summary results described herein are derived from the objects which they submitted at the end of testing.

Safelayer configured a PKI environment consisting of a Root CA, Subordinate CA and Sub Subordinate CA.

The following products has been tested:

- KeyOne® CA: the Certification Authority
- KeyOne® VA (former KeyOne® OCSP): the solution for verifying the status of a certificate, based on the OCSP protocol, before enabling transactions or accesses.
- KeyOne® Desktop: client applications for signing and ciphering files. It supports online certificate status validation and time stamping and it is compliant with Microsoft Outlook.

The following third party products where used:

- iPlanet Directory Server / repository was configured.
- Microsoft Outlook was the e-mail client used to conduct the tests.

A.6.2 Tests

A.6.2.1 Test Group 1 – Cross Certification

Safelayer conducted the following tests in this test group:

TEST 1 BASIC TEST - ROOT CA CROSS-CERTIFICATION

- Manual Method: Reference Root CA Certifies Participant Root CA
- Manual Method: Participant Root CA Cross Certifies Reference Root CA

Conclusion

Safelayer successfully demonstrated Mutual Cross-Certification of between the Safelayer Root CA and the Reference Root CA via the manual method, and contributed significantly to the test results through their detection of the following non-conformant issues in the reference system:

- “Incorrect encoding of Basic Constraints in End Entity Certificates issued by the Reference System”
- “Incorrect 160 bit SHA-1 hash”

A.6.2.2 Test Group 2 – Subordinate CA Certification

TEST 1 BASIC TEST - SUBORDINATE CA CERTIFICATION
Safelayer successfully concluded the following tests in this group:

- Manual Method: Reference Root CA Certifies Participant Subordinate CA
- Manual Method: Participant Subordinate CA Certifies Reference Sub Subordinate CA

Conclusion

Safelayer successfully performed the core tests within the Subordinate CA Certification test group, and contributed significantly to the test results through the detection of the following non-conformant issues in the reference system:

- "Incorrect encoding of Basic Constraints in End Entity Certificates issued by the Reference System"
- "Incorrect 160 bit SHA-1 hash"

A.6.2.3 Test Group 3 – Enrolment

Safelayer successfully performed the following tests in this test group:

- Manual method: Certification of User Generated Single Key Pair by Reference CA

Conclusion

Safelayer successfully completed the available tests in the Enrolment test group.

A.6.2.4 Test Group 4 – Certificate Validation and Path Construction

Conclusion

Safelayer successfully attempted tests in this test group and contributed significantly to the results by discovering several non-conformant issues in the Reference System:

- The extension accessLocation of the authorityInfoAccess is defined as a GeneralName type in the RFC2459/RFC3280 and RFC2560 but it is encoded as a GeneralNames by the Reference System. As it is a non-critical extension, the signed mail message could be verified.

A.7 SmartTrust/Nexus

A.7.1 Test Setup

SmartTrust/Nexus conducted online testing from their facility in Stockholm. The summary results described herein are derived from the document, which they submitted at the end of testing.

The product tested was **Certificate Manager 5**.
Siemens DirX version 6 server was used as the CA repository, but was not configured for external access via the MaxWare virtual directory.
Microsoft Outlook 2002 was the e-mail client used to conduct the tests.
An OCSP Responder was not configured.

SmartTrust/Nexus configured a PKI environment consisting of a Root CA and Subordinate CA.

A.7.2 Tests

A.7.2.1 Test Group 1 – Cross Certification

SmartTrust/Nexus conducted the following tests in this subgroup:

- Participant Root CA certifies Reference Root CA
- Reference Root CA certifies Participant Root CA

SmartTrust/Nexus conducted the Manual Mutual Cross-Certification, Mutual Trust between the Participant Root CA to the Reference Root CA tests in TG 1. The Manual Unidirectional Cross-Certifications in both directions were performed as steps to complete the Mutual Cross-Certification test.

Conclusion

SmartTrust/Nexus successfully performed Mutual Cross-Certification between the SmartTrust/Nexus Root CA and the Reference Root CA.

A.7.2.2 Test Group 2 – Subordinate CA Certification

SmartTrust/Nexus conducted the following tests:

- Participant Root CA certifies Reference Subordinate CA
- Reference Root CA certifies Participant Subordinate CA
- Participant Subordinate CA certifies Reference Sub-Subordinate CA
- Reference Subordinate CA certifies Participant Sub-Subordinate CA

Conclusion

SmartTrust/Nexus successfully completed the Subordinate CA Certification.

A.7.2.3 Test Group 3 – Enrolment

SmartTrust/Nexus successfully completed the following tests in this group:

Certification of User Generated single key pair by Reference CA

SmartTrust/Nexus demonstrated that their application could create a valid PKCS10 file which could be used by the Reference system to issue a certificate.

Conclusion

SmartTrust/Nexus successfully completed the core tests in this test group.

A.7.2.4 Test Group 4 – Certificate Validation and Path Construction

Conclusion

SmartTrust/Nexus did not perform any of the tests in this test group.

A.8 TC TrustCenter

A.8.1 Test Setup

TC TrustCenter conducted online testing from their facility in Germany.

The product tested was the TC TrustCenter Web RA.

A.8.2 Tests

A.8.2.1 Test Group 3 – Enrolment

TC TrustCenter conducted the following test in this group:

On-line Enrolment using Participant CA-side signing key generation and Participant CA-side encryption key generation

TC TrustCenter demonstrated enrolment to their CA using Microsoft Internet Explorer as the enrolment client.

S/MIME Compliance tests where conducted with Outlook 2000 (Reference side) and Mozilla 1.2 Messenger (Participant Side)

Conclusion

TC TrustCenter successfully demonstrated end-entity enrolment to their CA.

A.9 UTI Systems Romania

A.9.1 Test Setup

UTI Systems conducted online testing from their facility in Bucharest. The summary results described herein are derived from the document which they submitted at the end of testing.

The product tested was **CertSafe** version 1.2
The product tested was **Certificate Manager 5**.
OpenLDAP server was used as the CA repository.
Outlook Express was the e-mail client used to conduct the tests.
An OCSP Responder was not configured.

A.9.2 Tests

A.9.2.1 Test Group 1 – Cross Certification

UTI Systems conducted the following tests in this subgroup:

- Participant Root CA certifies Reference Root CA
- Reference Root CA certifies Participant Root CA

UTI Systems conducted the Manual Mutual Cross-Certification, and Mutual Trust between the Participant Root CA to the Reference Root CA in TG 1. The Manual Unidirectional Cross-Certifications in both directions were performed as steps to complete the Mutual Cross-Certification test.

Conclusion

UTI Systems successfully performed Mutual Cross-Certification between the UTI Systems Root CA and the Reference Root CA.

A.9.2.2 Test Group 2 – Subordinate CA Certification

UTI systems reported successful conduct of the following tests in this group:

- Participant Root CA certifies Reference Subordinate CA
- Reference Root CA certifies Participant Subordinate CA
- Reference Subordinate CA certifies Participant Sub Subordinate CA
- Participant Subordinate CA certifies Reference Sub Subordinate CA

Conclusion

UTI Systems successfully performed the core Subordinate Certification tests.

A.9.2.3 Test Group 3 – Enrolment

UTI Systems conducted the following tests in this group:

- Manual Certification of User Generated Single Key Pair by Reference CA
- Exchange signed e-mail with the Reference System

Conclusion

UTI Systems successfully performed the core Enrolment test and the e-mails exchange with the reference system.

A.9.2.4 Test Group 4 – Certificate Validation and Path Construction

Conclusion

UTI Systems did not perform any of the tests in this test group.

A.10 VeriSign - BTIgnite

A.10.1 Test Setup

VeriSign conducted online testing from the facility of BT Ignite, their UK Affiliate. The summary results described herein are derived from the documents and objects (certificates, pkcs10 etc.) which they submitted during testing.

The product tested was based on **Managed PKI version 5.0**
VeriSign´s directory service was used as the CA repository.
Microsoft Outlook 2000 was the e-mail client used to conduct the tests.
An OCSP Responder was configured but was not tested at this time.
A PKI Environment with a Root CA and Subordinate CA.

A.10.2 Tests

A.10.2.1 Test Group 1 – Cross Certification

VeriSign conducted the following tests in this subgroup:

- Participant Root CA certifies Reference Root CA
- Reference Root CA certifies Participant Root CA

VeriSign conducted Manual Mutual Cross-Certification between their Root CA and the Reference Root CA as part of the TG 1 interface tests. Manual Unidirectional Cross-Certifications in both directions were performed as steps to complete the Mutual Cross-Certification test.

Conclusion

VeriSign successfully performed Manual Mutual Cross-Certification between the VeriSign/BTIgnite Root CA and the Reference Root CA.

A.10.2.2 Test Group 2 – Subordinate CA Certification

VeriSign reported successful conduct of the following tests in this group:

- Participant Root CA certifies Reference Subordinate CA
- Reference Root CA certifies Participant Subordinate CA
- Reference Subordinate CA certifies Participant Sub Subordinate CA

Conclusion

VeriSign successfully performed the majority of the Subordinate CA Certification tests.

A.10.2.3 Test Group 3 – Enrolment

Conclusion

VeriSign did not perform any of the tests in this test group.

A.10.2.4 Test Group 4 – Certificate Validation and Path Construction

Conclusion

VeriSign did not perform any of the tests in this test group.

Annex B: Testing participants contact list

To obtain further details regarding the results for a particular organisation or more information about the /products please contact the following:

Baltimore	General	Jack Nagle Director Public Sector Marketing Tel: +353 1 881 6703 jnagle@baltimore.com
Cryptomathic	Test results	Eimear Gallery, Solutions Architect, Eimear.Gallery@cryptomathic.com, +44 (0) 79 86769880 Jonathan Tuliani, Technical Manager, Jonathan.Tuliani@cryptomathic.com, +44 (0) 1223 225358
	Products	Antonio Gerbino, Consultant, Antonio.Gerbino@cryptomathic.com +44 (0) 1223 224355
	General	http://www.cryptomathic.com/ +44 (0) 1223 225354
Guardeonic Solutions	Test results	Danny Wallace, Test Manager, danny.wallace@guardeonic.com
	Products	Emer O'Reilly, Product Manager, emer.oreilly@guardeonic.com
	General	info@guardeonic.com http://www.guareonic.com/
Microsoft	General	Steve Adler stevead@microsoft.com http://www.microsoft.com/
RSA	Test results	Hans Lorentzon, hlorentzon@rsasecurity.com, +44 1344 781719
	Products	Anna Philippen, aphilippen@rsasecurity.com, +44 1344 781 728
	General	http://www.rsasecurity.com/
Safelayer Secure Communications	General	Safelayer Secure Communications, S.A. Product Marketing <producto@safelayer.com> Ed. World Trade Center (S-4) Moll de Barcelona s/n 08039 Barcelona (Spain) Phone: +34 93 5088090 Fax: +34 93 5088091 http://www.safelayer.com/
SmartTrust/Nexus	General	Fredrik Cronholm, Configuration manager, fredrik.cronholm@nexus.se, Malin Ridelius, Product Manager, malin.ridelius@nexus.se http://www.nexus.se/ NB Development, maintenance and support of SmartTrust PKI products are managed by Technology Nexus AB. General information is available at: http://www.nexus.se/
TCTrustCenter	Test results	Thomas Blumenthal, Test Manager, thomas.blumenthal@trustcenter.de
	Products	Gunter Weinerth, Productmanager, gunter.weinerth@trustcenter.de
	General	info@trustcenter.de
UTI Systems	General	Mr. Mihai Ianciu IT&C Division Manager UTI Systems S.A. 31 Vasile Lascar St., Bucharest, Romania Phone: 004021 20.12.330 Fax: 004021 21. 10. 542 E-mail: mihai.ianciu@uti.ro
VeriSign Inc.	General	Gabriel Dusil Marketing Director, EMEA VeriSign Inc. Chemin de Blandonnet, 8

		CH-1214 Vernier, Geneva Switzerland Mobile: +44 (7712) 891-093 Fax: +44 (1483) 838-146 email: gdusil@verisign.com Web: http://www.verisign.com/
	Technical:	Paul Green Systems Engineer, EMEA VeriSign Inc. Chemin de Blandonnet, 8 CH-1214 Vernier, Geneva Switzerland Mobile: +44 (797) 407-1010 Business Fax: +44 (776) 489-0710 E-mail: pgreen@verisign.com http://www.verisign.com/

Table 7: Testing Participants Contact Details

Annex C: EEMA contact

To obtain further details about the pkiC you can contact:

EEMA	Project specific	Jane Hebson Jane.Hebson@eema.org Direct Line: +44 1527 837596 Office: +44 1386 793028
	Press and Marketing	Ruth Cattell Ruth.cattell@eema.org Direct line: +44 1384 374008 Direct fax: +44 7970 146369 EEMA - 'the Catalyst for e-Business in Europe' Alexander House, High Street, Inkberrow, Worcester. UK www.eema.org Registered in Brussels - reg. no. 6594/89 EEMA Tel. +44 1386 793028 EEMA Fax. +44 1386 793268

Table 8: EEMA Contact Details

Annex D: Presentations at conferences

2001

- TESI PCC Meeting, Italy, 24 January
- ECAF Seminar, Lisbon, 8 - 9 March
- PKI Forum, US, 13 - 15 March
- ISTC WP Meeting, Brussels, 29 March
- Infosec, London, 24 - 25 April
- Cosic Course, Belgium, 9 June
- EEMA Annual Meeting, Paris, 11 - 13 June
- PKI Forum, Germany, 21 June
- PKI Forum, US, 01 Sept
- ISSE Conf, London, 26 - 28 September
- ISSS WG/EC in Brussels
- RSA Implementation conference, Amsterdam, 15 November
- IP Security, London, December
- EEMA Government Interest Group Meeting, Paris, 6 December
- Hungary Conference, 13 December
- RANS Conference, Russia, 18 December

2002

- EEMA 2002, Amsterdam, 10 - 12 June
- ISSE October, October 2 - 4
- EEMA ECAF Meeting, London, 3 December

2003

- Infosecurity Press Briefing, London, January
- CompTIA Forum, Hatfield, UK, 5 February
- CompTIA Forum, Amsterdam, 6 February

Annex E: Press coverage

2001

- Silicon.com - January 8
  Million euro pledge to break PKI deadlock
- Silicon.com - January 18
  PKI investigation labelled a waste of time and money
- Computer User Daily News - 9 January
  PKI products to be interoperable within 2 years
- Total Telecom - 10 January
  EEMA launches e-commerce security challenge
- CW360 - 11 January
  EC project points finger at security vendors
- CW360 - 16 January
  RSA adds weight to pkiC
- Global Network Security Agencies (ESI) – August
  The pkiC (article in the name of Frank Jorissen)
- CW360 – June
  Complexity impedes e-Business security
- Computer Weekly – 21 June
  Complexity impedes e-Business security
- InfoSec Today - July
  The pkiC (article in the name of Frank Jorissen)
- Business International – September
  The pkiC (article in the name of Frank Jorissen)
- WMRC - Security Publication – September
  The pkiC (article in the name of Frank Jorissen)

2002

- Network News – 19 June
  Vendors keeping PKI all locked up
- Russian Magazine – June
  The pkiC
- IT Week - 17 June
  PKI leaders test interoperability
- Cyber Risk News – July
- EEMA pkiC
- Information Security Bulletin – July
- Testing PKI
- Database & Network Journal – August
- 15 security vendors sign-up to EEMA's pkiC
- Secure Computing – August
- EEMA's pkiC
- Computer Fraud and Security magazine – November
- PKI revelation of Key Problems

Updates and articles have also been in the

- monthly EEMA Online
- quarterly EEMA Briefings

Annex F: Acknowledgements

The following persons have actively contributed to the finalization of the final report:

- Steven Adler (Microsoft): review on the test results and technical recommendations
- Kevin Blackman (WISeKey): annex A and review technical recommendations
- Jordi Buch (Safelayer): review on the test results and technical recommendations
- David Chadwick (University of Salford): overall review and implications on standards and EU policies
- Chris Gilbert (Royal Mail): test environment description and test results
- Jane Hebson (EEMA): annex D and annex E
- Kate Hodgson (Royal Mail): overall review and technical recommendations
- David Hoyle (Microsoft): review on the test results and technical recommendations
- Chris Makemson (Security & Standards): project management chapters
- Patrick Paling (KPMG): Quality assurance
- Nick Pope (Security & Standards): overall review and implications on standards and EU policies
- Stefan Wijnen (Certipost – Begacom): report editor
- and to all the testing participants for their participation and the verification of the test results.

Annex G: Response to Review Recommendations

Three issues were raised as part of the formal review of the project carried out by the European Commission in July 2002. This Annex seeks to clarify how the Project Consortium believes the points have been addressed.

G.1 Cross-certification / SMIME client configuration

Review recommendation

"Cross-certification between different CAs is a problem solved in theory but that rarely works in COTS applications; provide details of how the S/MIME clients were configured in successful tests."

Project response

The reviewers were correct in identifying cross-certification and, therefore, certificate verification by the relying party as a problem. Although the mechanics of cross-certification were proved during the project, the issue of retrieving the certificates and CRLs from a "foreign" directory remains a major obstacle to the widespread use of PKI. A Virtual Directory was used as a work-round for this "directory problem" in the pkiC, in order to keep the scope of the project realistic and achievable.

However, the work-around is not suitable for industry use and the issue is still a major concern to the project consortium. This has been highlighted in the project deliverable "Challenges for the PKI Industry"[12].

Although email was used to prove some of the test results, testing S/MIME clients was specifically excluded from the project for a number of reasons: -

- to reduce complexity in the matrix of tests
- S/MIME testing had already been done as part of the CESG project
- tests were largely carried out by the Participants who did not provide information on the clients they used

G.2 LDAPv3

Review recommendation

"The tests use the LDAPv2 directory access protocol; since it is known that this version has problems with non-English character sets (e.g. in the DN) and with certificate and CRL search and retrieval, consider the option of running at least some test with LDAPv3, that is also much more common nowadays."

Project response

LDAPv2 was chosen as the lowest common denominator, in an attempt to make pair-wise testing possible between Participants. In the event, pair-wise testing did not happen because of time constraints. The project strongly recommends that all vendors should support LDAPv3, but recognises that, even had all the Participants been capable of using it, it would

[12] See section entitled "Certificate Dissemination"

not have addressed the major directory issues that still exist around certificate and CRL retrieval.

Lack of support for X.509 certificates, differing and incompatible directory schemas are defined as major industry issues in the paper, "Challenges for the PKI Industry". Recommended solutions include an industry standard LDAPv3 Schema for X.509 certificates and support for new extensions in RFC3280.[13]

G.3 Certificate content

Review recommendation

"Interoperability is often affected by certificate content (e.g. DN components, keyUsage bits), so detailed information should be available for interested technical users to understand which content format is preferred to maximize interoperability."

Project response

The recommendation has been fully met in this Final Report. The salient points have also been extracted into a separate paper, "pkiC – Guide for End Users", which makes recommendations on which configuration options should be used to maximise interoperability.

[13] See "LDAP" section

Annex H: Change History

Date	Version	Description	Change marked
2002/12/30	01	Initial partial draft of Admin Sections as sent to P. Paling for review of the structure	N/A
2003/01/20	02	Updated complete draft	N/A
2003/02/04	03	- Integrating the results of WP6 into this document - Creating missing chapters	N/A
2003/02/11	04	Update after conference call with pkiC consortium	N/A
2003/02/18	05	Update after review of the consortium members	N/A
2003/02/24	06	Updated with Conclusions & Recommendations in section 6.2.2	
2003/03/05	07	Updated with the results of a questionnaire to the participants and a rewritten annex	
2003/03/11	08	- Updated with latest information from J.Hebson and K.Blackman - Added a chapter about the directory system	
2003/03/19	09	- Reviewed and edited by D.Chadwick	Yes
2003/03/24	10	- Remarks from Microsoft - Remarks from N. Pope - Updated annex A and inserted annex B	Yes
2003/04/02	11	- Remarks from P. Paling - Small remarks from other reviewers	Yes
2003/04/02	12	New document structure	No
2003/04/07	13	Small corrections by K.Hodgson	No
2003/04/11	1.0	Final version by S.Wijnen	No
2003/04/15	1.1	Final editing by C. Makemson	Yes
2003/04/25	1.2	Further editing by J.Hebson and C .Makemson, also incorporating suggestions on section 4 from K.Hodgson and C.Gilbert	No
2003/04/25	1.3	Updates by C.Gilbert	Yes
2003/04/28	1.4	Checking and updating by C.Makemson	No
2003/04/30	1.4	Final update from comments by J.Hebson, S.Wijnen and K.Blackman	No
2003/04/30	1.5	Minor corrections	No
2003/05/12	1.6	Minor corrections resulting from Testing Participant comments	No
2003/05/20	1.7	Addition of annex addressing the Interim Review Recommendations	No