Federal Bridge Certification Authority (FBCA)
Path Discovery and Validation (PD-VAL)
Technical Working Group (TWG)
E-mail Exchange Demonstration (EED)
Test Plan and Results

December 2004

Prepared for the General Services Administration by

MTS™ Mitretek Systems

3150 Fairview Park Drive South
Falls Church, VA 22042-4519

TABLE OF CONTENTS

SECTION **PAGE**

LIST OF FIGURES

FIGURE **PAGE**

LIST OF TABLES

TABLE **PAGE**

SECTION 1

INTRODUCTION

1.1 BACKGROUND

The Federal Bridge Certification Authority (FBCA) is an information system that is currently one of the four CAs in the Federal PKI. The FPKI Operating Authority (OA) chairs two technical working groups: the FBCA TWG and the PD-VAL TWG. The latter makes recommendations on infrastructure and desktop solutions that will facilitate certificate validation using the FBCA. To support desktop solutions the PD-VAL TWG tested an e-mail exchange scenario (i.e., E-mail Exchange Demonstration – EED) using various PD VAL products.

1.2 PURPOSE AND SCOPE (WHAT IS TESTED)

This document describes the test procedure, testing activity, and test results of the EED project for the PD-VAL TWG. The purpose of this document is to enable other organizations to duplicate such EED testing and verify the results on their own.

The document is organized as follows.

Section 1 – Introduction – This section.

Section 2 – Assumptions and Goals – states the assumptions and the goal of EED testing

Section 3 – Methodology – Provides a description of the testing approach as well as the pass/fail criteria for EED

Section 4 – Testing Environment – Describes the testing environment, including hardware and software (i.e., Operating System(s) and applications).

Section 5 – Test Results and Findings to date – summarizes the results and explains the findings discovered during EED experimentation

Section 6 – Recommendation – discusses the recommendations based on the results of EED

Appendix A – Certificate Content Used for EED Testing– Provides contact information for obtaining the data files used in and generated by testing to-date, and for providing feedback on this project.

SECTION 2

ASSUMPTIONS AND GOAL

2.1 ASSUMPTIONS

The certificate of e-mail sender should be issued by a CA "on the other side of the FBCA" with respect to the trust anchor of the recipient. This means the CAs should be different, and should both be cross-certified with the FBCA.

2.1 GOALS

The goal of the EED testing is to test path discovery and validation supporting a signed e-mail application between users belonging to different trust domains cross-certified with the FBCA. The goal of the EED testing is verify the successful exchange of signed e-mail between FBCA participants, and between different software configurations of those participants. Specifically, e-mail is to be sent and received between agencies whose only trust relationship is via the FBCA, and with various combinations of Outlook both "out of the box," and as enhanced by the Entrust "Express" desktop validation product.

SECTION 3

METHODOLOGY

At a high level, there are four combinations for e-mail exchange between Microsoft Outlook with CAPI and Microsoft Outlook with Entrust Express 6.1, namely:

1. Microsoft → Entrust,
2. Microsoft → Microsoft
3. Entrust → Microsoft
4. Entrust → Entrust

However, in reality, things are more complicated.

This set of combinations could not be tested using simply 2 desktop machines (one Entrust and one Microsoft), because the same-platform tests (e.g., Microsoft → Microsoft) should have the sender and receiver on opposite sides of the FBCA. Our goal is to test path processing, so the sender and received machines must use different certificates, implying different desktop machines. Thus, four desktop machines are actually necessary – two for Microsoft, and two for Entrust.

Four machines give 16 possible combinations, with some repetition between the four high-level scenarios. When it was discovered that some of the 16 combinations that are in the same "scenario" have at times acted differently, for example, xp4 → xp1 (MS→MS) works, but xp1→xp4 (MS→MS) did not. It is clearly interesting to understand the differences between the 16 combinations even though they are at a finer grain than the 4 scenarios.

Sending messages from each of the four machines to each of the other four creates 16 different combinations summarized by the following "connectivity grid," shown in table 3-1.

Table 3-1 EED Testing Combinations

	sender			
recipient	**xp1**	**xp2**	**xp5**	**xp4**
xp1	Ms loop	Ent → Ms	Ent → Ms	Ms → Ms
xp2	Ms → Ent	Ent loop	Ent -> Ent	Ms → Ent
xp5	Ms → Ent	Ent → Ent	Ent loop	Ms → Ent loop
xp4	Ms → Ms	Ent → Ms	Ent → Ms loop	Ms loop

In table 3-1 “loop” refers to a condition where a message is being validated by relying party whose trust anchor is the same CA that issued the certificate that signed the message, thus bypassing path discovery. These “loop” conditions are not interesting from the path discovery and validation point-of-view, but can be revealing from the Application integration and certificate profile points-of-view (i.e. if they don’t work, one knows it is not a path processing problem).

3.1 APPROACH

Figure 3.1-1 depicts a high level diagram for the initial round of testing of the discovery and validation products in the EED project.

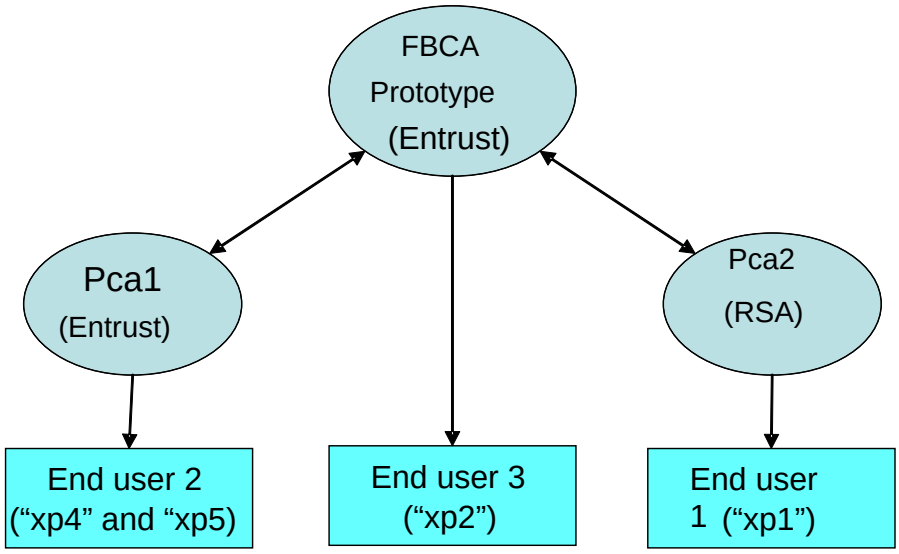

Figure 3.1-1 Certificate Topology

In figure 3.1-1 above Pca1, actually known as “o=ken pca, c=us,” is an Entrust CA cross certified with the FBCA Prototype. Pca1 is designed to directly create end users”, generally referred to hereafter as either as xp4 or xp5, that are named after the machines where the private keys for these end-user certificate are installed. Such xp4 or xp5 end-users have names along the lines of “cn=ken, o=ken pca, c=us.”

Pca2 in the above diagram, actually known as “ou=EgovProto1, ou=FBCA, o=U.S. Government, c=us” is a CA previously utilized as a TLS CA in EAuth related projects. It is an RSA CA configured to generate end-users, in this case with naming conventions such as

"E=stillson@mitretek.org, cn= stillson6, c=us". The EgovProto based end-user is generally referred to hereafter as "xp1."

For the purposes of testing shorter paths (which are sometimes easier), an unusual end-user certificate was generated directly from the FBCA prototype. This is "cn=Ken Stillson, ou=FBCAProto, ou=FBCA, o=U.S. Government, c=us," and generally referred to as "xp2."

All of the above CA's directories are X.500 chained; CA certificates should be retrievable from the LDAP directory fbcadir.mitertek.org.

3.2 TESTING TASKS

The test team will execute the tasks described below.

Establish a PKI with a certificate topology compatible with that shown in section 2.2, utilizing certificates profiles that will produce certificates with attributes similar to how found in the appendix

- Establish three issuing CAs cross certified with a single bridge. Utilize a mixture of Entrust and non-Entrust CA products
- Ensure that end-user and any intermediate CA certificates have AIA and CDP fields specified within the requirements given in section 5.1
- Load all CA certificates and cross-certificates into chained directories following the requirements in section 5.2

Install four Windows XP desktop machines configured as per table 4.2-1

- Two machines use Microsoft CAPI "out-of-the-box," using Office 2002, with both Windows and Office fully patched.
- Two machines utilize Entrust Express 6.1, using Office 2000, which should be fully patched prior to installation of Entrust Express.

Establish private keys and trust anchors as per table 4.2-1

- On the Entrust machines both the private keys and trust anchors are controlled by Entrust user profiles. Ensure that the profile for xp5 is "exportable," and export it into PKCS12 format after installation (for use on xp4).
- On the Microsoft machines, test anchors are established first by loading the trusted CA into the CAPI root store. Then PKCS12 files are loaded to establish private keys.

Configure Outlook

- The actual e-mail servers utilized are not important; it is possible for all four machines to share an e-mail server (and even an e-mail box); the IMAP is recommended if any sharing is used (although see notes in section 5 on IMAP and Entrust compatibility issues). In MTS's configuration, xp1 and xp2 share a mailbox, as do xp4 and xp5.
- The private key to be used in e-mail signing must be configured into Outlook before sending. If the certificate is not on the certificate selection list, see section 5.1.4.

Generate the sixteen e-mails combinations

- Generate a signed message from each of four machines sent to each of the four.

  All messages should be signed using S/MIME clear-text; this mode is a good common-denominator between Outlook and Entrust Express.

Clear caches

- If a previous test has been performed on the same machine, then clearing the caches will ensure than realistic path discovery is being performed on this iteration, rather than re-using previous partial results.

  For Outlook based systems – enter "Internet options" (right click on IE icon). On the "content" tab, select "Certificates," and select the "intermediate certificate authorities" tab. Select all certificates found and click "remove". Now "ok" back to Internet options, and select the "General" tab. Select "delete cookies" then "delete files" and turn on the "delete all offline content" option. This procedure appears to assure working from a clean slate.

  For Express – with Entrust logged out, delete all files find in the directory with Entrust's .epf file, other than the .epf file itself. This procedure will often cause a warning upon the next login (saying that information has been changed "outside of Entrust"), however this can be ignored, Entrust will automatically re-obtain this information from the Entrust CA.

Check the sixteen e-mail combinations

- If using IMAP on Entrust Express machines, copy-and-paste the messages into a local folder before opening. It appears that Express is not compatible with IMAP.
- Open each of the four e-mails on each of the four machines. Entrust Express will display a dialog with the results. In standard Outlook, click the red certificate tag to examine the results.

For each combination of the test case the test procedure followed is: (1) send a message; (2) open the message; (3) if success, end combination test; (4) if unsuccessful, find out why; then (5) if necessary, make changes to whatever parameter/profile and try again (i.e., go back to 1). This is done sixteen times to verify each element of the grid in Table 3-1.

3.2 TEST CASES

In the EED testing for the PD-VAL TWG there is only one test case (i.e., path processing based validation of signed e-mail) repeated sixteen times for sixteen different combinations of senders and recipients and their desktop machines.

3.3 PASS/FAIL AND SUSPENSION/RESUMPTION CRITERIA

The pass/fail criterion for the EED testing consists in verifying successful exchange of e-mail between all sixteen desktop machine combination pairs. To do this, one will open each of the four e-mails on each of the four machines. Upon failure, Entrust Express will display a dialog with the results; if no dialog box is displayed, validation was successful. In standard Outlook, click the red certificate tag to examine the results. Express pops up a dialog report with green or red check marks, whereas Outlook opens a box only upon a failure, it does nothing when it works.

SECTION 4

TESTING ENVIRONMENT

4.1 SYSTEM HARDWARE AND OPERATING SYSTEM (OS)

Testing out-of-the-box Microsoft Outlook validation (i.e., using the native Microsoft Cryptographic Application Programming Interface - CAPI) requires the utilization of Windows XP as the operating system, as only Windows XP currently supports path discovery and path validation out of the box. To simplify the number of combinations to test, Windows XP is used throughout the testing environment for all the relying party desktops, including the Entrust Express based ones that do not strictly require Windows XP.

To facilitate quick construction, replication, and making snap-shots of installations, all installations in the testing environment are actually using a virtual server system known as VMware Workstation, running on a Windows 2000 server host operating system. Several separate tests seem to have confirmed that all the tested scenarios and software operate identically in the virtual environment as on real machines, therefore the specifics of the host machine appear to not be relevant.

The host machine used in these tests is a Dell Optiplex EX GX270, with an Intel Pentium IV 2.60 GHz processor, 1GB of RAM, running Windows 2000 5.00.2195 service pack 4 with all critical OS updated as of 1/16/04 on a 30GB IDE hard disk, with the virtual machines stored on a 120GB IDE disk. VMware workstation version 4.0.5 is used.

Each of the virtual machines is running Windows XP version 2002, service pack 1, with all OS critical updates as of 3/19/04 installed. The virtual machines have been allotted 128 MB RAM, one 4 GB virtual hard-disk, and the ability to directly access the host machine's network card.

The hardware and operating systems of the CA computers is not discussed here, as only the certificate profiles of the CAs is believed to be of interest.

4.2 SYSTEM APPLICATIONS

The grid in table 4.2-1 summarizes the desktop and machine configurations for EED testing.

Table 4.2-1 EED Desktop Machine Applications

System name	MS Office version	Validation software	Certificate Issuer	Trust anchor(s)
xp1	2002 sp2	Microsoft CAPI	EGovProto1 (RSA)	EGovProto1
xp2	2002 sp2	Entrust Express 6.1	FBCA prototype	FBCA prototype
xp4	2002 sp2	Microsoft CAPI	Ken PCA 1 (Entrust)	Ken PCA1
xp5	2002 sp3	Entrust Express 6.1	Ken PCA 1 (Entrust)	Ken PCA1

Notes:

- Machines xp4 and xp5 utilize the same certificate (and thus same private key). This is to create a middle-ground between the Entrust and CAPI environments. Xp5 is an Entrust Express 6.1 machine using the Entrust CA generated certificate from Ken PCA1. The Entrust profile is exported from xp5 into a PKCS12 file, and imported into xp4, which runs Microsoft "out of the box." This creates a machine, xp4, that uses an Entrust-generated certificate, but within a CAPI environment, which turns out to be an interesting combination.

  It is worth noting that because there are four machines with only three certificates distributed among them, that 6 of the 16 combinations are "trivial" – meaning that the sender's certificate's issuer and the relying party's trust anchor are the same CA, in a few cases, they are even the same key. These trivial conditions are referred to in section 3 as 'loops'.

  While these trivial cases do not provide interesting tests results with respect to path processing, however, they are valuable as diagnostics for non-path processing errors, such as basic signature interoperability between Outlook and Entrust Express. Thus, these "trivial" cases are maintained in the testing grid.

  Xp5 was upgraded from Office 2002 service pack 2 to service pack 3 to ensure that the service pack level does not change the results.

SECTION 5

TEST RESULTS

Table 5-1 summarizes the EED testing result, as of the date of publication. Out of the sixteen combinations examined, two combinations failed, although only intermittently, and fourteen passed, although two only "conditionally"

Table 5-1 EED Test Result to date

	sender			
recipient	**xp1 (ms)**	**xp2 (ent)**	**xp5 (ent)**	**xp4 (ms)**
xp1 (ms)	(ok)	ok	ok	ok
xp2 (ent)	ok	(ok)	ok (time!)	ok (time!)
xp5 (ent)	ok	ok	(ok)	(ok)
xp4 (ms)	ok	ok	(ok)	(ok)

Table 5-1 uses a notation described in table 5-2 Condition key below.

Table 5-2 EED Test Result Condition Key

Condition	Description
(ok)	Works, but trivial loop-back trust
(time!)	Works, but takes a long time

The following subsections describe findings discovered during EED experimentation that might impact on E-Authentication program and FPKI implementation activities, such as profile development.

5.1 CERITICATE PROFILES FINDINGS

Experimentation has revealed that the exact certificate profile used for the sender / signer's certificate is critical to allowing the relying party to correctly perform path discovery and validation, especially when the relying party is Microsoft / CAPI out-of-the-box.

While it is the intention of the EED project to use "real" FBCA participant CAs for this purpose, it has been discovered that the certificate profile used to generate the sender's certificate is highly specific, and not compatible with current production profiles.

As a significant effort is required to change profiles for current test participants (Treasury and NFC), artificial CAs have been constructed for the initial round of testing in this project. It is expected that once the required profile requirements have been worked out with reasonable assurance, the FBCA PD-VAL technical working group will issue a profile document suitable for EED support and participation, and submit it to the Federal PKI Policy Authority for consideration.

An explanation of the profile requirements discovered thus far appear in the following subsections, and the certificate contents of the certificates used in the tests thus far are included in Appendix A.

5.1.1 AIA Fields

CAPI uses certificate Authority Information Access (AIA) "*caIssuers*" extensions during path discovery. This means that every certificate (end user and CA) must contain correctly populated AIA information. The most succinct description found thus far is this: an AIA field must point to the collection of all certificates whose subject matches the issuer of the certificate with the AIA field. This rule provides that not only should the issuer's certificate be available, but also all cross certificates issued to that CA.

The form of the AIA field is constrained. It must be either an HTTP URI that points to a PKCS 7 "bag of certificates", or a complete LDAP URI (with server-name specification) that points to an LDAP *caCertificate* attribute entries. CAPI will not parse cross certificate pairs – the individual cross certificates must be broken out and listed as *caCertificates*. Experimentation indicates that CAPI will only look at the first attribute value of an AIA field that successfully returns results, so it does not work to have one AIA entry that points to issuer certificate(s) and another that points to cross-certificates. For LDAP URIs, if the directory entry attribute itself is named with ";binary", then the URI must contain this appendage, and vice-versa; CAPI will not auto-detect the alternative.

5.1.2 CDP Fields

CAPI also requires that CRL distribution point (CDP) fields be populated for on-line status checks to be performed. A CDP must either be HTTP URI pointing to a .crl file, or a complete LDAP URI pointing to a *certificateRevocationList* attribute. CAPI appears to only use the first attribute value in a CDP field that returns a result (even an empty result). As with AIA field, for LDAP URIs, if the directory entry attribute itself is named with ";binary", then the URI must contain this appendage, and vice-versa; neither CAPI nor Entrust Express will not auto-detect the alternative.

5.1.3 CDP Entrust Complications

The current versions of Entrust CAs do not appear to be capable of generating CDP fields with the above format requirements. However, the Entrust CA is capable of importing a pre-calculated DER-encoded field. Mitretek created a small encoding tool for this purpose, and can make it available upon request. This works well in AIA fields, where the Entrust CA simply uses the provided encoded portion. Experiments have had mixed results with CDP fields; in some cases the provided DER segment is used as the CDP, but in some cases it is append, and becomes a 2nd CDP entry after the default (DN form) CDP. As CAPI only respects the first value in a CDP field, and the Entrust CA tends to put its DN form first, this creates CDPs that CAPI cannot consume. It appears that setting "Microsoft compatibility mode" was during CA installation allows correct operation.

5.1.4 CAPI E-mail Address Complications

CAPI will allow any private key to be imported, but Outlook does not always allow imported private keys to be used for e-mail signing. Different versions of Outlook and different OS and/or MS Office service packs appear to adjust the requirements.

In older versions, it appears that certificate subject DNs are required to contain an "email=" component that specifies an e-mail address that matches the e-mail address configured within Outlook. Newer versions will also allow a matching "subject alt-name" extension to qualify the certificate for signing. The exact cut-over between behaviors has not been determined. There are several registry entries (different entries for different versions of MS Office) which bypass these qualification checks and allow any private key to be used. Mitretek can provide information on these entries upon request. When Outlook decides that a certificate does not qualify for signing, it is simply not listed on the dialog box where the user selects a certificate for signing.

5.1.5 CAPI Policy Complications

It has been observed that if a certificate on a path asserts a disconnected policy, that is, a policy that is not mapped to-and-from neighboring certificates, that CAPI considers this an invalid path. This appears to be the case in multiple, if not all, OS and MS Office versions. The only solution found was to ensure that no CA asserts a disconnected policy (i.e. if any policies are asserted, make sure they are mapped during cross certification.)

5.1.6 Key IDs

It appears that CAPI requires correctly populated authority key ID's and subject key ID's when CA key rollover has occurred.

5.2 DIRECTORY PROFILES FINDINGS

Entrust Express does not utilize AIA (or SIA) fields for path discovery. It assumes that discovery can be performed by querying a directory for certificates needed to build the chain. This assumes that LDAP queries can be made against LDAP DNs that match the subject DNs of the certificates being sought. While it is common practice to match LDAP DNs and subject DNs for PKI objects, there is no standard that specifically requires this. Entrust Express does require this naming convention.

5.3 OUTLOOK FINDINGS

5.3.1 Trust Problems

Recent versions of Outlook, including Outlook 2003, include the self-signed certificate of the signer's trust chain when digitally signing S/MIME e-mail messages, and that the presence of this self-signed certificate prevents the recipient's Outlook from initiating path discovery, which would allow bridge-based trust to be discovered.

It is believed that some pre-path-discovery logic in Outlook notes that if it sees a self-signed cert in the chain, Outlook believes it can determine trust by simply checking whether that cert is in the local root store, and if not, it simply terminates the logic with "untrusted" without ever calling the Certificate.Build() method which could trigger path discovery.
A "design change request" was submitted to Microsoft to address this issue. Since that time, Microsoft has issued a "patch", the exsec32.dll file in the Office10 folder, should be replaced by the new exsec32.dll file. This patch allows Outlook to send digitally signed certificates without including the self signed certificate. Microsoft has released this "patch' formally as part of KB885232. Microsoft originally stated that there would be another patch that would

allow validation of certificates, even if the self-signed certificate is included in the message; however, they have since then stated that the testing effort required to ship a Windows QFE for Outlook/Outlook Express (this is a shared component) is very high and "will not meet the Windows QFE bar given the Outlook fix".

One other issue, which was untested during the EED, is a known bug that Microsoft's CAPI does not process name constraints properly without registry modifications. In order to resolve this, the process in Appendix B should be followed.

5.3.2 Protocol Problems

It also appears that the combination Entrust Express and Outlook 2002 ("xp") has compatibility issues with the IMAP protocol. While message validation will be performed, Outlook will frequently crash immediately after a validation operation has been performed on an IMAP based message. This condition can be avoided by coping-and-pasting the message from the IMAP INBOX folder into a locally stored folder. It is believed this issue does not arise for POP or Exchange based e-mail servers.

5.4 HOWTO: SETUP CAS AND CLIENTS TO SUPPORT PATH DISCOVERY AND VALIDATION

5.4.1 Entrust PKI CA

NOTE: The audience of this section is assumed to be capable of Entrust Administration.

- It does not work to have one AIA entry that points to issuer certificate(s) and another that points to cross-certificates, they must be in one entry for CAPI to process it.
- When issuing extensions it is important to note that for LDAP URIs (AIA and CDP), if the directory entry attribute itself is named with ";binary", then the URI must contain this appendage, and vice-versa; the applications will not auto-detect the alternative.

INSTALLING & CONFIGURING ENTRUST	
Installation	
1.	When configuring an Entrust CA, make sure to choose 'Microsoft compatibility mode' during configuration
Configuration of Certificate Profiles	
1.	Log into Entrust RA using Officer profile and password (created during installation)
2.	Click File...Certificate Definitions...Export (Master.certspec)

3.	Open Master.certspec (Notepad)
4.	For cross certificate, add the following to the appropriate sections (use correct DER encoded values, these are only an ***example***) ; ---------- ; Special Cross-Certificate Type Explicitly For FBCA prototype ; ---------- xcert_fbca=xcert,FBCAxcert,Cross-Certificates issued to FBCA [xcert_fbca Common Extensions] basicconstraints=2.5.29.19,c,m,DER,30030101FF; BasicConstraints w/cA = TRUE auth_info_access=1.3.6.1.5.5.7.1.1,n,m,DER,3081DB306806082B0601050507300 2865C6C6461703A2F2F666263616469722E6D6974726574656B2E6F72672F 6F753D4642434150726F746F2C6F753D464243412C6F3D552E532E20476F7 665726E6D656E742C633D55533F6341436572746966669636174653B62696E 617279306F06082B06010505073002866 36C6461703A2F2F6662636164697 22E6D6974726574656B2E6F72672F6F753D4642434150726F746F2C6F753D 464243412C6F3D552E532E20476F7665726E6D656E742C633D55533F63726 F737343657274696669636174655061697 23B62696E617279
5.	For default end user certificates (only if using Entrust Client), add the following to the appropriate sections (use correct DER encoded values, these are only an ***example***) [ent_default Common Extensions] auth_info_access=1.3.6.1.5.5.7.1.1,n,m,DER,3081DB306806082B0601050507300 2865C6C6461703A2F2F666263616469722E6D6974726574656B2E6F72672F 6F753D4642434150726F746F2C6F753D464243412C6F3D552E532E20476F7 665726E6D656E742C633D55533F6341436572746966669636174653B62696E 617279306F06082B06010505073002866 36C6461703A2F2F6662636164697 22E6D6974726574656B2E6F72672F6F753D4642434150726F746F2C6F753D 464243412C6F3D552E532E20476F7665726E6D656E742C633D55533F63726 F737343657274696669636174655061697 23B62696E617279
6.	For exportable end user certificates (only if using Microsoft or other client), add the following to the appropriate sections (use correct DER encoded values, these are only an ***example***) [ent_export Common Extensions] ;---------- ;- Exportable Enterprise Certificate Type - ;- - ;- This certificate type includes the certificate extension required - ;- by Entrust clients to allow them to export the corresponding -

	;- private key. - ;---------- privkeyexportable=2.16.840.1.114027.30.1,n,m,UTF8String,"The private key corresponding to this certificate may have been exported. "auth_info_access=1.3.6.1.5.5.7.1.1,n,m,DER,3081DB306806082B0601050507300 2865C6C6461703A2F2F666263616469722E6D6974726574656B2E6F72672F 6F753D4642434150726F746F2C6F753D464243412C6F3D552E532E20476F7 665726E6D656E742C633D55533F6341436572746966669636174653B62696E 617279306F06082B0601050507300286636C6461703A2F2F6662636164697 22E6D6974726574656B2E6F72672F6F753D4642434150726F746F2C6F753D 464243412C6F3D552E532E20476F7665726E6D656E742C633D55533F63726 F737343657274696669636174655061697 23B62696E617279
7.	Open entmgr.ini (*Ex. c:/authdata/manager/entmgr.ini*)
8.	Add the following (use correct URIs, these are only an example) [CDP] 1=*http://cam.mitretek.org/cadist/fbcaproto_cdp.crl* 2=*ldap://fbcadir.mitretek.org/ou=FBCAProto,ou=FBCA,o=U.S. Government,c=US?certificateRevocationList*
9.	Save and close entmgr.ini
Certificate Issuance	
1.	If using Microsoft as the client; Open Security Policy→ User Policy→ End User Policy (or alternate end user policy), ensure “Allow PKCS#12 export”, “CAPI Export”, and “CAPI Key export” are all checked
2.	Save changes
3.	When issuing a new user certificate, ensure the email section under the naming tab is filled in correctly
4.	If using *Microsoft* client, under the Certificate Information tab, ensure the export type (or equivalent) is used If using an *Entrust* client, under the Certificate Information tab, ensure the default type (or equivalent) is used
5.	Under General tab, ensure the appropriate end user policy is chosen (see Step 1)

5.4.2 RSA Keon CA

NOTE: The audience of this section is assumed to be capable of RSA Keon CA Administration.

- It does not work to have one AIA entry that points to issuer certificate(s) and another that points to cross-certificates, they must be in one entry for CAPI to process it.

- When issuing extensions it is important to note that for LDAP URIs (AIA and CDP), if the directory entry attribute itself is named with ";binary", then the URI must contain this appendage, and vice-versa; CAPI will not auto-detect the alternative.

INSTALLING & CONFIGURING RSA KEON	
End User Certificate Issuance	
1.	Ensure the following extension are highlighted; Authority information access Authority key identifier CRL distribution points Key usage Subject alternative names Subject key identifier
2.	Ensure the authInfoAccess is using a URI
3.	Ensure cRLDistPoints is set to distributionPoint, fullname and uses URI
4.	Ensure subjectAltNames is set to rfc822Name
5.	Enter the access method OID for authInfoAccess as 1.3.6.1.5.5.7.48.2
6.	Extensions should be inserted in the following format (these are only an example) authInfoAccess: Access method OID: 1.3.6.1.5.5.7.48.2 ldap://fbcadir.mitretek.org/ou=EgovProto1,ou=FBCA,o=U.S. Government,c=US?cACertificate;binary cRLDistPoints: ldap://fbcadir.mitretek.org/ou=EgovProto1,ou=FBCA,o=U.S. Government,c=US?certificateRevocationList;binary subjectAltNames: john.doe@acme.com
Cross-Certificate Issuance	
1.	Ensure the following extension are highlighted; Authority information access Authority key identifier Basic Constraints CRL distribution points Key usage Subject key identifier
2.	Ensure the authInfoAccess is using a URI
3.	Ensure cRLDistPoints is set to distributionPoint, fullname and uses URI

4.	Enter the access method OID for authInfoAccess as 1.3.6.1.5.5.7.48.2
5.	Extensions should be inserted in the following format (these are only an example) authInfoAccess: Access method OID: 1.3.6.1.5.5.7.48.2 ldap://fbcadir.mitretek.org/ou=EgovProto1,ou=FBCA,o=U.S. Government,c=US?cACertificate;binary cRLDistPoints: ldap://fbcadir.mitretek.org/ou=EgovProto1,ou=FBCA,o=U.S. Government,c=US?certificateRevocationList;binary

5.4.3 Entrust Express Client

- Machines must utilize Entrust Express 6.1, using Office 2000, which is fully patched prior to installation of Entrust Express.
- All messages should be signed using S/MIME clear-text.
- Entrust Express is not compatible with IMAP, use POP.

5.4.4 Outlook

- Windows XP, service pack 1, with all OS critical updates as of 3/19/04 must be used as the operating system, as only Windows XP currently supports path discovery and path validation out of the box.
- Machines must use Microsoft CAPI "out-of-the-box," using Office 2002, with both Windows and Office fully patched.
- If using an Entrust CA, ensure that the end-user profile is "exportable," and export it into PKCS12 format after installation.
- Trust anchors (CA Certificates) are established first by loading the trusted CA into the CAPI root store. Then PKCS12 files are loaded to establish private keys.
- The private key to be used in e-mail signing must be configured into Outlook before sending.
- All messages should be signed using S/MIME clear-text.

5.4.5 Architecture

- Directories should house, not only self signed CA certificates in the cACertificate attribute, but also all cross certificates issued to that CA (CAPI will not parse cross certificate pairs).
- For LDAP URIs (AIA and CDP), if the directory entry attribute itself is named with ";binary", then the URI must contain this appendage, and vice-versa; CAPI will not auto-detect the alternative.

SECTION 6

RECOMMENDATION

The PD-VAL WG recommends that other e-mail clients with validation functionality be sought until agencies former versions of Microsoft Windows are upgraded to Windows XP or to such a time when Microsoft provides path discovery functionality in previous versions of Windows.

If Microsoft XP is used for its path discovery and validation functionality it is important to remember the following:

1. CAPI will stop path validation if it encounters a self-signed certificate and there are no plans to correct this. In order to force Microsoft to send digitally signed e-mails without including the self-signed certificates, the KB885232 patch must be applied to all clients.

2. In order to process name constraints correctly, the procedures in Appendix B must be followed on all clients.

3. CAPI requires that AIA and CDP extensions are populated in all certificates in a path. More information on this can be found under section 5.1

4. CAPI will not validate certificates using CRLs that were signed with a different key. This will limit a client's ability to validation certificate paths which include a CA that has performed key rollover and has not reissued the certificates using the new key.

APPENDIX A

CERTIFICATE CONTENT USED FOR EED TESTING

A.1. xp1 certificate (from RSA CA):

```
 Certificate:
        Version: 3 (0x2)
        Serial Number:
            00BF FDA5 D4D1 AB2B 07C8 EB4F 556F 189F AA
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=us, O=U.S. Government, OU=FBCA, OU=EgovProto1
        Validity
            Not Before: Wednesday, October 06, 2004 12:01:13 PM
            Not After : Saturday, June 13, 2009 2:31:13 PM
        Subject: C=US, O=U.S. Government,OU=FBCA,OU=EgovProto1point4,
emailAddress=stillson@mitretek.org
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Authority Key Identifier:
                keyid:12 79 b1 17 df b6 bf 77 ca ca 95 f9 bf 1d de c2 95 e2 bf c7
            X509v3 Subject Key Identifier:
                15 0f fd bd 66 0f 32 3b 36 93 56 d7 47 77 99 bd 64 39 d7 fc
       X509v3 Subject Alternative Name:
                email:stillson@mitretek.org
            X509v3 CRL Distribution Points:
                URI:ldap://fbcadir.mitretek.org/cn OU=EgovProto1,ou=FBCA,o=U.S.
Government,c=US?certificateRevocationList
            Authority Information Access:
                CA Issuers - URI: ldap://fbcadir.mitretek.org/cn
OU=EgovProto1,ou=FBCA,o=U.S. Government,c=US?cACertificate
    Signature Algorithm: sha1WithRSAEncryption
```

A.2 xp2 certificate (from Entrust CA)

```
 Certificate:
        Version: 3 (0x2)
        Serial Number: 3E37 3BA9
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=U.S. Government, OU=FBCA, OU=FBCAProto
        Validity
            Not Before: Wednesday, September 22, 2004 1:36:39 PM
            Not After : Saturday, September 22, 2007 2:06:39 PM
        Subject: C=US, O=U.S. Government, OU=FBCA, OU=FBCAProto, CN=Stillson AIA6
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage:
                Digital Signature
            X509v3 Private Key Usage Period:
                Not Before: Wednesday, September 22, 2004 1:36:39 PM, Not After:
Sunday, October 29, 2006 12:06:39 AM
            2.16.840.1.114027.30.1:
                .IThe private key corresponding to this certificate may have been
exported.
            Authority Information Access:
                CA Issuers - URI:ldap://fbcadir.mitretek.org
/ou=FBCAProto,ou=FBCA,o=U.S. Government,c=US?cACertificate;binary
                CA Issuers - URI:ldap://fbcadir.mitretek.org
/ou=FBCAProto,ou=FBCA,o=U.S. Government,c=US?crossCertificatePair;binary
            X509v3 Subject Alternative Name:
                email:stillson@mitretek.org
            X509v3 CRL Distribution Points:
                DirName:/C=US/O=U.S. Government/OU=FBCA/OU=FBCAProto/CN=CRL1
                URI:http://cam.mitretek.org/cadist/fbcaproto_cdp.crl
                URI:ldap://fbcadir.mitretek.org/ou=FBCAProto,ou=FBCA,o=U.S.
Government,c=US?certificateRevocationList
            X509v3 Authority Key Identifier:
                KeyID=4f a4 7c 13 92 80 bb eb 50 34 da 0b 05 d7 51 1b ba c4 6f 4b
            X509v3 Subject Key Identifier:
                29 95 16 05 1e 70 1e ff 5f 24 4f 84 26 52 14 6f 09 28 08 1b
            X509v3 Basic Constraints:
                Subject Type=End Entity
            1.2.840.113533.7.65.0:
                0 ..V6.0....
    Signature Algorithm: sha1WithRSAEncryption
```

Note the order of the CDP field entries – this can cause warnings when received under native Microsoft, on occasion, only the first entry is checked, and the first entry is an X.500 form that Microsoft cannot process. Ideally, X.500 form CDPs should not be first.

Note that the AIA field order is “correct” – the caCertificates attribute (which Microsoft can process) is first. The crossCertificatePair attribute (which Microsoft doesn’t process) is 2nd.

A.3 xp5 and xp4 certificate (from Entrust)

```
Certificate:
        Version: 3 (0x2)
        Serial Number: 3FC3 65A3
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=Ken PCA
        Validity
            Not Before: Wednesday, September 22, 2004 1:25:20 PM
            Not After : Saturday, September 22, 2007 1:55:20 PM
        Subject: C=US, O=Ken PCA, CN=KenCA User18
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
        X509v3 extensions:
            X509v3 Key Usage:
                Digital Signature
            X509v3 Private Key Usage Period:
                Not Before: Wednesday, September 22, 2004 1:25:20 PM, Not After: Saturday,
October 28, 2006 11:55:20 PM
            2.16.840.1.114027.30.1:  .IThe private key corresponding to this
certificate may have been exported.
            Authority Information Access:
                CA Issuers –
            URI:ldap://fbcadir.mitretek.org/ou=FBCAProto,ou=FBCA,o=U.S.
Government,c=US?cACertificate;binary
            URI:ldap://fbcadir.mitretek.org/ou=FBCAProto,ou=FBCA,o=U.S.
Government,c=US?cACertificate;binary
            X509v3 Subject Alternative Name:
                email:ken@tsf.mitretek.org
            X509v3 CRL Distribution Points:
                DirName:/C=US/O=Ken PCA/CN=CRL1
                URI:ldap://fbcadir.mitretek.org/ou=FBCAProto,ou=FBCA,o=U.S.
Government,c=US?certificateRevocationList
                URI:http://cam.mitretek.org/cadist/kenpca_cdp.crl
            X509v3 Authority Key Identifier:
                KeyID=39 14 fc 3f 07 b7 37 f5 77 f0 17 d7 0b 67 32 a7 56 64 85 b7
            X509v3 Subject Key Identifier:
                44 c2 b3 db ff ce f9 b2 d0 26 30 ed 80 50 e0 f5 55 9c dd 6f
            X509v3 Basic Constraints:
                Subject Type=End Entity
            1.2.840.113533.7.65.0: 0..V7.0....
    Signature Algorithm: sha1WithRSAEncryption
```

Note the order of the CDP field entries – this can cause warnings when received under native Microsoft, on occasion, only the first entry is checked, and the first entry is an X.500 form that Microsoft cannot process. Ideally, X.500 form CDPs should not be first.

A.4 xp1 issuer: “EGovProto1” self-signed

```
Certificate:
     Version: 3 (0x2)
     Serial Number:
         0085 C7E3 6588 A68E 0760 5CFD 2E6A 1080 E1
     Signature Algorithm: sha1WithRSAEncryption
     Issuer: C=us, O=U.S. Government, OU=FBCA, OU=EgovProto1
     Validity
         Not Before: Thursday, June 17, 2004 2:28:29 PM
         Not After : Thursday, June 16, 2009 2:28:29 PM
     Subject: C=us, O=U.S. Government, OU=FBCA, OU=EgovProto1
     Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
         RSA Public Key: (1024 bit)
             Modulus (1024 bit):
             Exponent: 65537 (0x10001)
     X509v3 extensions:
         X509v3 Basic Constraints: critical
             CA:TRUE
         X509v3 Key Usage: critical
             Digital Signature, Non Repudiation, Certificate Sign, CRL Sign
         X509v3 Certificate Policies:
             Policy: 2.16.840.1.101.3.2.1.48.5
         X509v3 Authority Key Identifier:
             KeyID=12 79 b1 17 df b6 bf 77 ca ca 95 f9 bf 1d de c2 95 e2 bf c7
         X509v3 Subject Key Identifier:
             12 79 b1 17 df b6 bf 77 ca ca 95 f9 bf 1d de c2 95 e2 bf c7
 Signature Algorithm: sha1WithRSAEncryption
```

A.5 xp2 issuer: The FBCA Prototype

```
Certificate:
        Version: 3 (0x2)
        Serial Number: 1043804375 (0x3e3730d7)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=U.S. Government, OU=FBCA, OU=FBCAProto
        Validity
            Not Before: May 30 10:59:36 2003 GMT
            Not After : May 30 11:29:36 2013 GMT
        Subject: C=US, O=U.S. Government, OU=FBCA, OU=FBCAProto
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            Netscape Cert Type:
                SSL CA, S/MIME CA, Object Signing CA
            X509v3 CRL Distribution Points:
                DirName:/C=US/O=U.S. Government/OU=FBCA/OU=FBCAProto/CN=CRL1
            X509v3 Private Key Usage Period:
                Not Before: May 30 10:59:36 2003 GMT, Not After: May 30 11:29:36
2013 GMT
            X509v3 Key Usage:
                Certificate Sign, CRL Sign
            X509v3 Authority Key Identifier:
                keyid:4F:A4:7C:13:92:80:BB:EB:50:34:DA:0B:05:D7:51:1B:BA:C4:6F:4B
            X509v3 Subject Key Identifier:
                4F:A4:7C:13:92:80:BB:EB:50:34:DA:0B:05:D7:51:1B:BA:C4:6F:4B
            X509v3 Basic Constraints:
                CA:TRUE
            1.2.840.113533.7.65.0:
                0...V6.0:4.0....
    Signature Algorithm: sha1WithRSAEncryption
```

A.6 xp4 and xp5 issuer: Ken PCA1

```
 Certificate:
        Version: 3 (0x2)
        Serial Number: 1069767172 (0x3fc35a04)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=Ken PCA
        Validity
            Not Before: Nov 25 13:08:29 2003 GMT
            Not After : Nov 25 13:38:29 2023 GMT
        Subject: C=US, O=Ken PCA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            Netscape Cert Type:
                SSL CA, S/MIME CA, Object Signing CA
            X509v3 CRL Distribution Points:
                DirName:/C=US/O=Ken PCA/CN=CRL1
            X509v3 Private Key Usage Period:
                Not Before: Nov 25 13:08:29 2003 GMT, Not After: Nov 25 13:38:29
2023 GMT
            X509v3 Key Usage:
                Certificate Sign, CRL Sign
            X509v3 Authority Key Identifier:
                keyid:39:14:FC:3F:07:B7:37:F5:77:F0:17:D7:0B:67:32:A7:56:64:85:B7
            X509v3 Subject Key Identifier:
                39:14:FC:3F:07:B7:37:F5:77:F0:17:D7:0B:67:32:A7:56:64:85:B7
            X509v3 Basic Constraints:
                CA:TRUE
            1.2.840.113533.7.65.0: 0...V6.0:4.0....
    Signature Algorithm: sha1WithRSAEncryption
```

A.7 cross certificate from FBCA Proto to EGovProto1

```
Certificate:
        Version: 3 (0x2)
        Serial Number: 3E37 3BCE
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=U.S. Government, OU=FBCA, OU=FBCAProto
        Validity
            Not Before: Monday, September 27, 2004 10:02:10 AM
            Not After : Thursday, September 27, 2007 10:32:10 AM
        Subject: C=us, O=U.S. Government, OU=FBCA, OU=EgovProto1
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            Authority Information Access:
                CA Issuers - URI:
ldap://fbcadir.mitretek.org/ou=FBCAProto,ou=FBCA,o=U.S.
Government,c=US?cACertificate;binary
                CA Issuers - URI:
ldap://fbcadir.mitretek.org/ou=FBCAProto,ou=FBCA,o=U.S.
Government,c=US?crossCertificatePair;binary
            X509v3 CRL Distribution Points:
                DirName:/C=US/O=U.S. Government/OU=FBCA/OU=FBCAProto/CN=CRL1
                URI: http://cam.mitretek.org/cadist/fbcaproto_cdp.crl
                URI:ldap://fbcadir.mitretek.org:389/ou=FBCAProto,ou=FBCA,o=U.S.
Government,c=US?certificateRevocationList
            X509v3 Key Usage:
                Certificate Sign, CRL Sign
            X509v3 Authority Key Identifier:
                KeyID=4f a4 7c 13 92 80 bb eb 50 34 da 0b 05 d7 51 1b ba c4 6f 4b
            X509v3 Subject Key Identifier:
                12 79 b1 17 df b6 bf 77 ca ca 95 f9 bf 1d de c2 95 e2 bf c7
            1.2.840.113533.7.65.0:
                0..V6.0....
    Signature Algorithm: sha1WithRSAEncryption
```

Note the order of the CDP field entries – this can cause warnings when received under native Microsoft, on occasion, only the first entry is checked, and the first entry is an X.500 form that Microsoft cannot process. Ideally, X.500 form CDPs should not be first.

A.8 cross certificate from EGovProto1 to FBCA Proto

```
Certificate:
        Version: 3 (0x2)
        Serial Number:
            00E8 3264 DFB7 3570 E581 4841 D0A9 A98D BB
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=us, O=U.S. Government, OU=FBCA, OU=EgovProto1
        Validity
            Not Before: Monday, September 27, 2004 10:30:36 AM
            Not After : Saturday, June 13, 2009 2:30:36 PM
        Subject: C=US, O=U.S. Government, OU=FBCA, OU=FBCAProto
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Authority Key Identifier:
                KeyID=12 79 b1 17 df b6 bf 77 ca ca 95 f9 bf 1d de c2 95 e2 bf c7
            X509v3 CRL Distribution Points:
                URL=LDAP://fbcadir.mitretek.org/ou=EgovProto1,ou=FBCA,o=U.S.
Government,c=US?certificateRevocationList;binary
            Authority Information Access:
                CA Issuers -
URL=LDAP://fbcadir.mitretek.org/ou=EgovProto1,ou=FBCA,o=U.S.
Government,c=US?cACertificate;binary
            X509v3 Basic Constraints
                CA:TRUE
            X509v3 Subject Key Identifier:
                4f a4 7c 13 92 80 bb eb 50 34 da 0b 05 d7 51 1b ba c4 6f 4b
                    Signature Algorithm: sha1WithRSAEncryption
```

A.9 cross certificate from FBCA Proto to Ken PCA1

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 3E37 3BCD
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=U.S. Government, OU=FBCA, OU=FBCAProto
        Validity
            Not Before: Monday, September 27, 2004 10:01:19 AM
            Not After : Thursday, September 27, 2007 10:31:19 AM
        Subject: C=US, O=Ken PCA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            Authority Information Access:
                CA Issuers - URI:ldap:// fbcadir.mitretek.org
/ou=FBCAProto,ou=FBCA,o=U.S. Government,c=US?cACertificate;binary
                CA Issuers - URI:ldap:// fbcadir.mitretek.org
/ou=FBCAProto,ou=FBCA,o=U.S. Government,c=US?crossCertificatePair;binary
            X509v3 CRL Distribution Points:
                DirName:/C=US/O=U.S. Government/OU=FBCA/OU=FBCAProto/CN=CRL1
                URL=http://cam.mitretek.org/cadist/fbcaproto_cdp.crl
                URI:ldap://fbcadir.mitretek.org:389/ou=FBCAProto,ou=FBCA,o=U.S.
Government,c=US?certificateRevocationList
            X509v3 Key Usage:
                Certificate Sign, CRL Sign
            X509v3 Authority Key Identifier:
                keyid:4F:A4:7C:13:92:80:BB:EB:50:34:DA:0B:05:D7:51:1B:BA:C4:6F:4B
            X509v3 Subject Key Identifier:
                39:14:FC:3F:07:B7:37:F5:77:F0:17:D7:0B:67:32:A7:56:64:85:B7
            1.2.840.113533.7.65.0:
                0 ..V6.0....
    Signature Algorithm: sha1WithRSAEncryption
```

Note the order of the CDP field entries – this can cause warnings when received under native Microsoft, on occasion, only the first entry is checked, and the first entry is an X.500 form that Microsoft cannot process. Ideally, X.500 form CDPs should not be first.

A.10 cross certificate from Ken PCA1 to FBCA Proto

```
Certificate:
        Version: 3 (0x2)
        Serial Number: 3FC3 65EB
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=Ken PCA
        Validity
            Not Before: Monday, September 27, 2004 9:41:56 AM
            Not After : Thursday, September 27, 2007 10:11:56 AM
        Subject: C=US, O=U.S. Government, OU=FBCA, OU=FBCAProto
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            Authority Information Access:
                CA Issuers - URI:ldap://fbcadir.mitretek.org/o=Ken
PCA,c=US?cACertificate;binary
                CA Issuers - URL=ldap://fbcadir.mitretek.org/o=Ken
PCA,c=US?crossCertificatePair;binary
            X509v3 CRL Distribution Points:
                DirName:/C=US/O=Ken PCA/CN=CRL1
                URL=ldap://fbcadir.mitretek.org/o=Ken
PCA,c=US?certificateRevocationList
                URL=http://cam.mitretek.org/cadist/kenpca_cdp.crl
            X509v3 Key Usage:
                Certificate Sign, CRL Sign
            X509v3 Authority Key Identifier:
                KeyID=39 14 fc 3f 07 b7 37 f5 77 f0 17 d7 0b 67 32 a7 56 64 85 b7
            X509v3 Subject Key Identifier:
                4f a4 7c 13 92 80 bb eb 50 34 da 0b 05 d7 51 1b ba c4 6f 4b
               1.2.840.113533.7.65.0:  0 ..V6.0....
    Signature Algorithm: sha1WithRSAEncryption
```

Note the order of the CDP field entries – this can cause warnings when received under native Microsoft, on occasion, only the first entry is checked, and the first entry is an X.500 form that Microsoft cannot process. Ideally, X.500 form CDPs should not be first.

APPENDIX B

REGISTRY ENTRY TO CORRECT WINDOWS NAME CONSTRAINTS PROCESSING

CryptoAPI Policy Options

Windows Server 2003, Windows XP SP2, and Windows 2000 SP5 (when released) clients support the following policy options on the local machine that may be set in the registry as DWORD values in the following location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SystemCertificates\Root\ProtectedRoots
```

The following values are bitmask values that may be added and applied to the above registry key (using the entry *Flags*) to affect the local machine policy:

- 0x1 – Disable user root store trust. This will prevent CryptoAPI applications from using the user root store in building trusted certificate chains.
- 0x2 – Disable user root store changes. This will prevent the user from adding root CAs to the user trusted root store. This value may be also set through Group Policy in Windows Server 2003.
- 0x4 – Disable user root store purge. This will prevent the user from removing root CAs from the user trusted store that are also the local machine trusted root store.
- 0x10 – Disable the requirement for NTAuth policy processing. This will disable the requirement for an issuing CA to be present in the NTAuth store of the local machine. This value may be set via group policy. In Windows Server 2003.
- 0x20 – Disable name constraint enforcement for undefined name types. By default, Windows XP SP2 and Windows Server 2003 will reject undefined name types in a name constraint validation. Setting this value will accept all name forms that are not explicitly defined.

LIST OF REFERENCES

1. Draft Federal Public Key Infrastructure Directory Profile, Version 2.5 (draft), 8 October 2002, http://www.cio.gov/fbca/documents/fpki_directory_profile.pdf
2. Authentication and Identity Policy Framework For Federal Agencies, version v.1.0, http://www.cio.gov/ficc/documents/FICCframework.pdf
3. International Telecommunications Union – Telecommunications Sector (ITU T) Recommendation X.509 (1997) | ISO/IEC 9594 8: 1997, “Information technology - Open Systems Interconnection - The Directory: Authentication framework”, June 1997.
4. International Telecommunications Union – Telecommunications Sector (ITU T) Recommendation X.521 (1997) | ISO/IEC 9594-7: 1997, “Information technology - Open Systems Interconnection - The Directory: Selected object classes.

The following Internet RFCs have been identified as sources of schema information:

5. RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile. R. Housley, W. Ford, W. Polk, D. Solo. April 2002. (Format: TXT=278438 bytes) (Obsoletes RFC2459) (Status: PROPOSED STANDARD)

6. RFC 1777: Lightweight Directory Access Protocol. W. Yeong, T. Howes, S. Kille. March 1995. (Format: TXT=45459 bytes) (Obsoletes RFC1487) (Status: DRAFT STANDARD)

7. RFC 2251: Lightweight Directory Access Protocol (v3). M. Wahl, T. Howes, S. Kille. December 1997. (Format: TXT=114488 bytes) (Status: PROPOSED STANDARD)

8. RFC 2559: Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2. S. Boeyen, T. Howes, P. Richard. April 1999. (Format: TXT=22889 bytes) (Updates RFC1778) (Status: PROPOSED STANDARD)

9. RFC 2587: Internet X.509 Public Key Infrastructure LDAPv2 Schema. S. Boeyen, T. Howes, P. Richard. June 1999. (Format: TXT=15102 bytes) (Status: PROPOSED STANDARD)

10. RFC 2798: Definition of the inetOrgPerson LDAP Object Class. M. Smith. April 2000. (Format: TXT=32929 bytes) (Status: INFORMATIONAL)

11. RFC 3494: Lightweight Directory Access Protocol version 2 (LDAPv2) to Historic Status. K. Zeilenga. March 2003. (Format: TXT=9225 bytes) (Obsoletes RFC1484, RFC1485, RFC1487, RFC1777, RFC1778, RFC1779, RFC1781, RFC2559) (Status: INFORMATIONAL)

The following RFCs are included by reference in the above mentioned RFCs:

12. RFC 1274: The COSINE and Internet X.500 Schema. P. Barker, S. Kille. November 1991. (Format: TXT=92827 bytes) (Status: PROPOSED STANDARD)

13. RFC 2079: Definition of an X.500 Attribute Type and an Object Class to Hold Uniform Resource Identifiers (URIs). M. Smith. January 1997. (Format: TXT=8757 bytes) (Status: PROPOSED STANDARD)

14. RFC 2256: A Summary of the X.500(96) User Schema for use with LDAPv3. M. Wahl. December 1997. (Format: TXT=32377 bytes) (Status: PROPOSED STANDARD)

15. RFC 3377: Lightweight Directory Access Protocol (v3): Technical Specification. J. Hodges, R. Morgan. September 2002. (Format: TXT=9981 bytes) (Updates RFC2251, RFC2252, RFC2253, RFC2254, RFC2255, RFC2256, RFC2829, RFC2830) (Status: PROPOSED STANDARD)

GLOSSARY OF TERMS AND ACRONYMS

CAPI	Crypographic Application Programming Interface – The Microsoft interface to its cryptographic services
CA	Certification Authority
DN	Distinguished Name
HTTP	Hyper Text Transfer Protocol
LDAP	Lightweight Directory access protocol