

CertAgent® 5.5.0 Release Notes

/******\

Information in this document is subject to change without notice and does not represent a commitment on the part of Information Security Corp. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of the agreement. The purchaser may make one copy of the software for backup purposes. No part of this manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose other than the purchaser's personal use without the prior written permission of Information Security Corp.

CertAgent is commercial computer software and, together with any related documentation, is subject to the restrictions on U.S. Government use as set forth below.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software Clause at DFARS 52.227-7013. "Contractor/manufacturer" is Information Security Corporation, 1141 Lake Cook Road, Suite D, Deerfield, IL 60015, U.S.A.

CertAgent is a registered trademark of Information Security Corp. and is protected by U.S. Patents No. 5,274,707; 5,373,560; 5,699,431

Copyright(c) 1999-2008 Information Security Corporation.
All rights reserved.

This document was last modified on: August 8, 2008

/******/

Table of Contents

1	Version 5.5.0	4
1.1	Enhancements and Modifications	4
1.1.1	RMI Change	4
1.1.2	CA Account Enhancements.....	4
1.1.3	Public Site	4
1.1.4	Registration Authority Management Interface (RAMI)	4
1.1.5	CACLI Enhancements.....	4
1.1.6	Databases.....	5
1.1.7	LDAP	5
1.2	Known Bugs, Limitations, and Workarounds	6
1.2.1	Custom Extensions	6
1.2.2	Certificate Extensions.....	6
1.2.3	Browser-based Enrollment and Certificate Retrieval	6
1.2.4	Renewing Certificates in Internet Explorer on Vista.....	6
1.2.5	Path Validation Issue with Renewed Issuer Certificates	7
2	Version History	8
2.1	Version 5.4.0.....	8
2.1.1	CA Account Enhancements.....	8
2.1.2	Registration Authority Management Interface (RAMI)	8
2.1.3	CACLI Enhancements.....	8
2.1.4	Known Bugs, Limitations, and Workarounds	9
2.2	Version 5.3.0.....	10
2.2.1	CA Account Enhancements.....	10
2.2.2	Registration Authority Management Interface (RAMI)	10
2.2.3	CACLI Enhancements.....	10
2.2.4	DBAccess Service	10
2.2.5	Known Bugs, Limitations, and Workarounds	11
2.3	Version 5.2.0.....	11
2.3.1	CA Account Enhancements.....	12
2.3.2	Key Management Utility	12
2.3.3	Certificate Report Generator	12
2.3.4	Certificate Database	12
2.3.5	DBAccess Service	12
2.3.6	Known Bugs, Limitations, and Workarounds	12
2.4	Version 5.1.0.....	13
2.4.1	New Version Requirement for Java Runtime Environment	13
2.4.2	System Configuration Change.....	13
2.4.3	Server Start-Up Changes	14
2.4.4	Changes to Administrative Site	14
2.4.5	CA Account Enhancements.....	14
2.4.6	Public Site Changes.....	15
2.4.7	CACLI Enhancements.....	15
2.4.8	New DBAccess Service.....	15
2.4.9	Known Bugs, Limitations, and Workarounds	15
2.5	Version 5.0.0.....	16
2.5.1	Server Start-Up.....	16
2.5.2	Administrative Site.....	16
2.5.3	CA Accounts	17
2.5.4	Public Site	17
2.5.5	Key Management Utility	18
2.5.6	Command Line Program	18
2.5.7	Bulk Enrollment Interface	18

2.5.8	Databases.....	18
2.5.9	Bug Fixes.....	18
2.5.10	Known Bugs, Limitations, and Workarounds	19
2.6	Version 4.3.0.....	19
2.6.1	CA Accounts	19
2.6.2	Public Site	20
2.6.3	Key Management Utility	20
2.6.4	Certificate Report Generator	20
2.6.5	Bug Fixes.....	20
2.6.6	Known Bugs, Limitations, and Workarounds	20
2.6.7	Plans for the Next Release.....	21
2.7	Version 4.2.0.....	21
2.7.1	Administrative Site.....	21
2.7.2	CA Accounts	21
2.7.3	Public Site	22
2.7.4	Bug Fixes.....	23
2.7.5	Known Bugs, Limitations, and Workarounds	23
2.7.6	Plans for the Next Release.....	23
2.8	Version 4.1.1	24
2.8.1	CA Accounts	24
2.8.2	Known Bugs, Limitations, and Workarounds	24
2.9	Version 4.1.0.....	24
2.9.1	CA Accounts	24
2.9.2	Public Site	26
2.9.3	Key Management Utility	26
2.9.4	Command-line Utilities	26
2.9.5	Java Interface.....	27
2.9.6	LDAP	27
2.9.7	Known Bugs, Limitations, and Workarounds	27
2.10	Version 4.0.0.....	27
2.10.1	Installation.....	27
2.10.2	Administrative Site.....	28
2.10.3	CA Account Site.....	28
2.10.4	Public Site	28

1 Version 5.5.0

1.1 Enhancements and Modifications

1.1.1 RMI Change

- 1.1.1.1 RMI connections are now restricted to allow localhost access only. Consequently the ability to run the public site on one or more alternate systems is no longer supported. (This feature may be added back into a future release with appropriate authentication mechanisms required between the two components.)

1.1.2 CA Account Enhancements

- 1.1.2.1 Each master account user can now finely control the rights of authorized users of subordinate sub-accounts:
 - a new 'Rights' tab on the sub-account settings page contains six sub-tabs that provide rights configuration settings for sub-accounts; the sub-tabs are labeled 'Account Status', 'Certificate Requests', 'Certificates', 'CRLs', 'Preferences', and 'Audit Trail'
- 1.1.2.2 Configuration settings for the number of contact e-mail address fields to display and the number of unique e-mail addresses each user is required to enter into the public enrollment form are now available; master accounts and sub-accounts have separate controls for these settings.
- 1.1.2.3 Added support for keys based on more than one elliptic curve to be accepted in certificate requests; changed the default setting for acceptable ECC key types to NIST P-256 and NIST P-384 (as recommended for Suite B compatibility purposes).
- 1.1.2.4 Updated the available action items on the Certificate | Advanced page
- 1.1.2.5 Moved the settings 'Allow default certificate issuance settings to be overridden' and 'Allow CRL issuance options' from a sub-account's 'General' configuration page to its 'Rights - Certificate Requests' and 'CRLs' tabs respectively.

1.1.3 Public Site

- 1.1.3.1 Depending on the CA account configuration settings, zero or more contact e-mail address fields will be displayed on enrollment forms.
- 1.1.3.2 When searching for certificates by e-mail address, the system will attempt to find the supplied search string within the `subjectDN` and `subjectAlternativeName` of each certificate.

1.1.4 Registration Authority Management Interface (RAMI)

- 1.1.4.1 RAMI only honors a request for certificate issuance, revocation, or reinstatement, or CRL issuance from a sub-account if the sub-account has the corresponding rights granted to it by its superior master account.

1.1.5 CACLI Enhancements

- 1.1.5.1 Feature and syntax updates:
 - added a `-rights` option to display the rights of a sub-account when used with the `-showconf -subca` command
- 1.1.5.2 Configuration file changes to `default-ca-conf.txt` and `default-subca-conf.txt`:
 - updated enrollment page sections
 - added contact e-mail address sections

- 1.1.5.3 Changes to 'default-subca-conf.txt':
- o added 'rights' section
 - o removed `right.override.cert` and `right.issueCRL` values

1.1.6 Databases

- 1.1.6.1 Renamed all databases files from '*db500.*' to '*db550.*'
- 1.1.6.2 Updated certificate database schema:
- o added an "EMAIL" column in which to store the e-mail addresses found in each certificate's `subjectDN` and `subjectAlternativeName`

1.1.7 LDAP

- 1.1.7.1 Rather than returning as the MAIL attribute of a certificate the first e-mail address found in `subjectDN`, all e-mail addresses found in `subjectDN` and `subjectAlternativeName` are returned
- 1.1.7.2 If values for the RDNs O, OU, T and/or C are found in `subjectDN`, they are now returned in the attributes COMPANY, DEPARTMENT, TITLE and CO, respectively, as well as in the attributes O, OU, T and C, resp., as in previous releases.

1.2 Known Bugs, Limitations, and Workarounds

1.2.1 Custom Extensions

- 1.2.1.1 **WARNING:** No validation checks are performed on custom extensions; whatever values are supplied are treated as opaque blobs and simply inserted into the issued certificates.

1.2.2 Certificate Extensions

- 1.2.2.1 **Limitation:** The delimiters ‘!’, ‘|’, ‘^’ may not appear in the values of any of the following certificate fields and extensions:

- certificate RDNs
- issuer alternative name
- subject alternative name
- authority information access
- CRL distribution points
- certificate policies
- name constraints

This limitation will be addressed in a future release.

1.2.3 Browser-based Enrollment and Certificate Retrieval

- 1.2.3.1 Netscape 4.7 (without Personal security Manager (PSM)) is not supported.

- 1.2.3.2 Netscape 4.7 (with Personal security Manager (PSM)): when installing a newly issued certificate and chain from the certificate retrieval page, CA certificates are not automatically imported.

Workaround: Use the link named “Install the CA certificate(s) into your certificate store” to import any missing issuer certificates.

- 1.2.3.3 Netscape 7.0: when viewing a newly issued certificate, the browser may display the warning “Could not verify this certificate because the issuer is not trusted.”

Workaround: Select the root CA certificate in the Authorities section of the certificate store. Click Edit and check all the trust settings. Then, click OK to apply your changes.

- 1.2.3.4 Mozilla Firefox 1.5: when installing a newly issued certificate and chain from the certificate retrieval page, CA certificates are not automatically imported.

Workaround: Use the link named “Install the CA certificate(s) into your certificate store” to import any missing issuer certificates.

- 1.2.3.5 Internet Explorer on Vista: when installing a newly issued certificate and chain from the certificate retrieval page, the root CA certificate is not automatically imported into CAPI’s “Trusted Root Certificate Authorities” store.

Workaround: Download the root CA certificate and manually import it into CAPI’s “Trusted Root Certificate Authorities” store before installing the certificate chain.

1.2.4 Renewing Certificates in Internet Explorer on Vista

- 1.2.4.1 Due to a feature change in Microsoft’s CAPICOM library for Vista, ‘renewed’ certificates are not properly associated with existing private keys upon import.

Workaround: At this time the only workaround we can suggest is to not allow certificate renewal or to use a non-Vista system to mediate the update process as follows:

1. on the Vista system, export your old certificate and its private key to a PKCS#12 file
2. move that file to a non-Vista system and import it into Netscape, Firefox, or Internet Explorer
3. open CertAgent's certificate retrieval page in this same browser and click the link to install your renewed certificate (the non-Vista system will properly associate this certificate with the private key imported from the .p12 file in step 2)
4. export the renewed certificate and its associated private key to a second PKCS#12 file
5. move the second PKCS#12 file back to your Vista system and import it into Internet Explorer

ISC's Credential Management Utility (CMU) can, of course, be used to automate this procedure to a reasonable degree.

1.2.5 Path Validation Issue with Renewed Issuer Certificates

- 1.2.5.1 Browsers (other than Internet Explorer) and other applications that build certificate validation paths by matching the authority key identifier extension in a subject's certificate with the subject key identifier in the issuer's certificate may regard as invalid any certificate issued by a CertAgent CA whose certificate has been 'renewed' (as their authority key identifier value will have changed). While Internet Explorer does not appear to suffer from this problem, it may be best to avoid using the certificate renewal process for CAs issuing certificates that may be used with other browsers.

2 Version History

2.1 Version 5.4.0

2.1.1 CA Account Enhancements

- 2.1.1.1 Added support for custom extensions: extensions not explicitly supported on the certificate issuance pages can be added to the certificate.
 - ‘Custom’ tab added to the Certificate Issuance page accepts base64-encoded custom extension
 - ‘Custom Extensions’ sections were also added to the ‘Generate Root CA Certificate’ and ‘Advanced Certificate Request’ pages
- 2.1.1.2 subjectAlternativeName and issuerAlternativeName extensions now accept otherName types with hex-encoded values.

2.1.2 Registration Authority Management Interface (RAMI)

- 2.1.2.1 The RAMI configuration page was simplified by removing the individual ‘allow override’ options (for subject DN, keyUsage, subjectDirectoryAttribute, and subjectAlternativeName extensions) and replacing them with a single “Allow POST to override default settings” option.
- 2.1.2.2 If the “Allow POST to override default settings” option is enabled, it is left to the RA’s discretion to use POST parameters to replace, or append to, default certificate issuance settings for the corresponding CA account
- 2.1.2.3 Certificate requests lacking a subject e-mail address are no longer rejected even when “Class 1 assurance” is enabled in the GUI; it is assumed that the RA itself can perform whatever low assurance e-mail address checking is required
- 2.1.2.4 As it assumes the RA can more easily perform these services if they are required, the RAMI no longer:
 - screens for duplicates even if “check for certificate request duplication” is enabled in the GUI
 - notifies the CA by e-mail after receiving a request even if such e-mail notifications are enabled in the GUI
 - notifies the user after processing a request even if such e-mail notifications are enabled in the GUI
- 2.1.2.5 Updated RAMI post parameters and status code
- 2.1.2.6 Updated RAMI sample program

2.1.3 CACLI Enhancements

- 2.1.3.1 Feature and syntax updates:
 - added `-certcustom` option to display default custom extensions when using `-showconf`
- 2.1.3.2 Configuration file updates (default-ca-conf.txt)
 - updated `rami.keyEnrollment` available value
- 2.1.3.3 Configuration files (default-ca-conf.txt, default-subca-conf.txt and cakey-conf-sample.txt) have been updated to:
 - accept hex-encoded values for otherName types in subjectAlternativeName and issuerAlternativeName extensions
 - added `cert.ext.custom` for custom extensions

2.1.4 Known Bugs, Limitations, and Workarounds

2.1.4.1 Custom Extensions

- **WARNING:** No validation checks are performed on custom extensions; whatever values are supplied are treated as opaque blobs and simply inserted into the issued certificates.

2.1.4.2 Certificate Extensions

- **Limitation:** The delimiters '!', '|', '^' may not appear in the values of any of the following certificate fields and extensions:
 - certificate RDNs
 - issuer alternative name
 - subject alternative name
 - authority information access
 - CRL distribution points
 - certificate policies
 - name constraints

This limitation will be addressed in a future release.

2.1.4.3 Browser-based Enrollment

- Netscape 4.7 (without Personal security Manager (PSM)): not supported
- Netscape 4.7 (with Personal security Manager (PSM)): when installing a newly issued certificate and chain from the certificate retrieval page, CA certificate(s) are not automatically imported

Workaround: Use the “Install the CA certificate(s) into your certificate store” link to import any missing CA certificates.

- Netscape 7.0: when viewing a newly issued certificate in certificate store, it displays the warning “Could not verify this certificate because the issuer is not trusted.”

Workaround: Select the root CA certificate in the Authorities section of the certificate store. Click Edit and check all the trust settings. Then, click OK to save the changes.

- Mozilla Firefox 1.5: when installing a newly issued certificate and chain from the certificate retrieval page, CA certificate(s) are not automatically imported

Workaround: Use the “Install the CA certificate(s) into your certificate store” link to import any missing CA certificates.

- Internet Explorer on Vista: when installing a newly issued certificate and chain from the certificate retrieval page, the root CA certificate is not automatically imported into CAPI's “Trusted Root Certificate Authorities” store

Workaround: Download root certificate and manually import it into CAPI's “Trusted Root Certificate Authorities” store before installing the certificate chain.

2.1.4.4 Renewing Certificates in Internet Explorer on Vista

- Due to a feature change in Microsoft's CAPICOM library for Vista, ‘renewed’ certificates are not properly associated with existing private keys upon import.

Workaround: At this time the only workaround we can suggest is to not allow certificate renewal or to use a non-Vista system to mediate the update process as follows:

1. on the Vista system, export your old certificate and its private key to a PKCS#12 file
2. move that file to a non-Vista system and import it into Netscape, Firefox, or Internet Explorer
3. open CertAgent's certificate retrieval page in this same browser and click the link to install your renewed certificate (the non-Vista system will properly associate this certificate with the private key imported from the .p12 file in step 2)
4. export the renewed certificate and its associated private key to a second PKCS#12 file

5. move the second PKCS#12 file back to your Vista system and import it into Internet Explorer

ISC's Credential Management Utility (CMU) can, of course, be used to automate this procedure to a reasonable degree.

2.1.4.5 Path Validation Issue with Renewed Issuer Certificates

- o Browsers (other than Internet Explorer) and other applications that build certificate validation paths by matching the authority key identifier extension in a subject's certificate with the subject key identifier in the issuer's certificate may regard as invalid any certificate issued by a CertAgent CA whose certificate has been 'renewed' (as their authority key identifier value will have changed). While Internet Explorer does not appear to suffer from this problem, it may be best to avoid using the certificate renewal process for CAs issuing certificates that may be used with other browsers.

2.2 Version 5.3.0

2.2.1 CA Account Enhancements

- 2.2.1.1 Allow certificates without basicConstraints to be added to an account ACL

2.2.2 Registration Authority Management Interface (RAMI)

- 2.2.2.1 Renamed Bulk Enrollment Interface (BEI) to Registration Authority Management Interface (RAMI)

- 2.2.2.2 Support certificate revocation and reinstatement and CRL issuance along with enrollment; these capabilities are configurable via the web-interface and CACLI program

- 2.2.2.3 Support CRMF request on key enrollment

- 2.2.2.4 If "posted entire subject DN overrides the default RDN setting" option is enabled, posted "subject" value will be used as the issued certificate DN rather than the subject DN of the posted certificate request

- 2.2.2.5 Updated RAMI post parameters and status code

2.2.3 CACLI Enhancements

- 2.2.3.1 Feature and syntax updates:

- o renamed `-bulkenroll` option to `-rami` when using `-showconf` and `-addacl`
- o renamed `-certmanagement` option to `-revocationpolicy` when using `-showconf`
- o added `-removeacl` option to remove a certificate from the ACL for a CA account or sub-account

- 2.2.3.2 Configuration file updates (default-ca-conf.txt)

- o renamed `cert.bulkenrollment` to `rami.keyEnrollment`
- o added `rami.certificateRevocation` and `rami.crlIssuance` for configuration of the certificate revocation/reinstatement and CRL issuance options in the registration authority management interface (formerly called the BEI)

2.2.4 DBAccess Service

- 2.2.4.1 Updated SELECT statement syntax: `SELECT (([LIMIT <offset> <limit>] (<columns> | *)) | COUNT(*)) FROM ENTRY [WHERE <expression>] [ORDER BY <column> [ASC | DESC]]`

- o support `LIMIT <offset> <limit>` to return specified number of rows in a query
- o support `COUNT(*)` to return number of rows in a query
- o accept `*` as column name to return all columns in a row

2.2.5 Known Bugs, Limitations, and Workarounds

2.2.5.1 Browser-based Enrollment

- Netscape 4.7 (without Personal security Manager (PSM)): not supported
- Netscape 4.7 (with Personal security Manager (PSM)): when installing a newly issued certificate and chain from the certificate retrieval page, CA certificate(s) are not automatically imported

Workaround: Use the “Install the CA certificate(s) into your certificate store” link to import any missing CA certificates.

- Netscape 7.0: when viewing a newly issued certificate in certificate store, it displays the warning “Could not verify this certificate because the issuer is not trusted.”

Workaround: Select the root CA certificate in the Authorities section of the certificate store. Click Edit and check all the trust settings. Then, click OK to save the changes.

- Mozilla Firefox 1.5: when installing a newly issued certificate and chain from the certificate retrieval page, CA certificate(s) are not automatically imported

Workaround: Use the “Install the CA certificate(s) into your certificate store” link to import any missing CA certificates.

- Internet Explorer on Vista: when installing a newly issued certificate and chain from the certificate retrieval page, the root CA certificate is not automatically imported into CAPI’s “Trusted Root Certificate Authorities” store

Workaround: Download root certificate and manually import it into CAPI’s “Trusted Root Certificate Authorities” store before installing the certificate chain.

2.2.5.2 Renewing Certificates in Internet Explorer on Vista

- Due to a feature change in Microsoft’s CAPICOM library for Vista, ‘renewed’ certificates are not properly associated with existing private keys upon import.

Workaround: At this time the only workaround we can suggest is to not allow certificate renewal or to use a non-Vista system to mediate the update process as follows:

1. on the Vista system, export your old certificate and its private key to a PKCS#12 file
2. move that file to a non-Vista system and import it into Netscape, Firefox, or Internet Explorer
3. open CertAgent’s certificate retrieval page in this same browser and click the link to install your renewed certificate (the non-Vista system will properly associate this certificate with the private key imported from the .p12 file in step 2)
4. export the renewed certificate and its associated private key to a second PKCS#12 file
5. move the second PKCS#12 file back to your Vista system and import it into Internet Explorer

ISC’s Credential Management Utility (CMU) can, of course, be used to automate this procedure to a reasonable degree.

2.2.5.3 Path Validation Issue with Renewed Issuer Certificates

- Browsers (other than Internet Explorer) and other applications that build certificate validation paths by matching the authority key identifier extension in a subject’s certificate with the subject key identifier in the issuer’s certificate may regard as invalid any certificate issued by a CertAgent CA whose certificate has been ‘renewed’ (as their authority key identifier value will have changed). While Internet Explorer does not appear to suffer from this problem, it may be best to avoid using the certificate renewal process for CAs issuing certificates that may be used with other browsers.

2.3 Version 5.2.0

2.3.1 CA Account Enhancements

- 2.3.1.1 Enhanced searching and reporting for certificate requests:
 - added “revocation date” and “not before date” as search criteria
 - removed “last modified date”
 - renamed “expiration date” to “not after date”
- 2.3.1.2 During key generation for a root CA, a PKCS#8 PDU (with null password) containing the new private key is created in RAM, encrypted under the system certificate, and then written to disk. (Previous versions used a temporary disk file.)

2.3.2 Key Management Utility

- 2.3.2.1 Supports HSM-based key generation

2.3.3 Certificate Report Generator

- 2.3.3.1 Updated “-date” option to support searching on revocation, not before, and not after dates
- 2.3.3.2 Updated “-sort” option to support sorting on revocation, not before, and not after dates

2.3.4 Certificate Database

- 2.3.4.1 Updated database schema
 - added “NotBeforeDate” column to store certificates’ not before dates
 - renamed “LastModDate” column to “RevocationDate”; the value of this field will be null for a valid certificate, changed to the revocation date when the certificate is revoked or put on hold, and reset to null when the status of an on-hold certificate is changed back to valid
 - renamed “ExpiredDate” to “NotAfterDate”

2.3.5 DBAccess Service

- 2.3.5.1 RMI registry connections are now secured using SSL/TLS with client authentication
- 2.3.5.2 Updated DBAccess API
 - Client credential info is now passed in as arguments to the class DBAccess constructor; credentials stored in a Java keystore file, in a PKCS#12 file, or on an HSM are supported
 - renamed the “getResult” method to “executeQuery”
 - added an “executeUpdate” method that accepts SQL “CREATE INDEX...” or “DROP INDEX...” statements to support index creation and deletion

2.3.6 Known Bugs, Limitations, and Workarounds

- 2.3.6.1 Browser-based Enrollment
 - Netscape 4.7 (without Personal security Manager (PSM)): not supported
 - Netscape 4.7 (with Personal security Manager (PSM)): when installing a newly issued certificate and chain from the certificate retrieval page, CA certificate(s) are not automatically imported

Workaround: Use the “Install the CA certificate(s) into your certificate store” link to import any missing CA certificates.

 - Netscape 7.0: when viewing a newly issued certificate in certificate store, it displays the warning “Could not verify this certificate because the issuer is not trusted.”

Workaround: Select the root CA certificate in the Authorities section of the certificate store. Click Edit and check all the trust settings. Then, click OK to save the changes.

- Mozilla Firefox 1.5: when installing a newly issued certificate and chain from the certificate retrieval page, CA certificate(s) are not automatically imported

Workaround: Use the “Install the CA certificate(s) into your certificate store” link to import any missing CA certificates.

- Internet Explorer on Vista: when installing a newly issued certificate and chain from the certificate retrieval page, the root CA certificate is not automatically imported into CAPI’s “Trusted Root Certificate Authorities” store

Workaround: Download root certificate and manually import it into CAPI’s “Trusted Root Certificate Authorities” store before installing the certificate chain.

2.3.6.2 Renewing Certificates in Internet Explorer on Vista

- Due to a feature change in Microsoft’s CAPICOM library for Vista, ‘renewed’ certificates are not properly associated with existing private keys upon import.

Workaround: At this time the only workaround we can suggest is to not allow certificate renewal or to use a non-Vista system to mediate the update process as follows:

6. on the Vista system, export your old certificate and its private key to a PKCS#12 file
7. move that file to a non-Vista system and import it into Netscape, Firefox, or Internet Explorer
8. open CertAgent’s certificate retrieval page in this same browser and click the link to install your renewed certificate (the non-Vista system will properly associate this certificate with the private key imported from the .p12 file in step 2)
9. export the renewed certificate and its associated private key to a second PKCS#12 file
10. move the second PKCS#12 file back to your Vista system and import it into Internet Explorer

ISC’s Credential Management Utility (CMU) can, of course, be used to automate this procedure to a reasonable degree.

2.3.6.3 Path Validation Issue with Renewed Issuer Certificates

- Browsers (other than Internet Explorer) and other applications that build certificate validation paths by matching the authority key identifier extension in a subject’s certificate with the subject key identifier in the issuer’s certificate may regard as invalid any certificate issued by a CertAgent CA whose certificate has been ‘renewed’ (as their authority key identifier value will have changed). While Internet Explorer does not appear to suffer from this problem, it may be best to avoid using the certificate renewal process for CAs issuing certificates that may be used with other browsers.

2.4 Version 5.1.0

2.4.1 New Version Requirement for Java Runtime Environment

- 2.4.1.1 JRE 1.5 or above is now required for proper operation of CertAgent (JRE 1.4.x is no longer supported)

2.4.2 System Configuration Change

- 2.4.2.1 A session timeout value for both admin and CA accounts can now be specified using the Java system property ‘isc.ca.web.session.timeout’; the default timeout value is 30 minutes

2.4.3 Server Start-Up Changes

- 2.4.3.1 Added an option to prompt for the system password using a dialog box when using the command line to start the server (`-prompt` with `-gui`); use this when `-prompt` alone fails to display on your terminal (as may happen on some system when using `nohup` to run the command line)

2.4.4 Changes to Administrative Site

- 2.4.4.1 Audit trail improvements:
- updated viewer: the user can now filter the events to be displayed by specifying a date range (options: today only, last 7 days, last 30 days, or custom 'from/to' dates)
 - added 'logout due to session time out' event
- 2.4.4.2 CA certificates in PKCS#7 files are now ignored when installing end-user certificates into the ACLs for admin and CA accounts

2.4.5 CA Account Enhancements

- 2.4.5.1 Independent settings are now accepted for the frequency of automatic CRL issuance and CRL validity periods (*i.e.*, the time increments used to compute `nextUpdate` fields); this change provides additional flexibility in allowing each new CRL to be issued automatically at a pre-set time interval prior to expiration of the preceding CRL
- 2.4.5.2 The bulk enrollment interface (BEI) for each CA account now has its own TLS ACL independent of the web access ACL for that account
- 2.4.5.3 The option to supply a self-management password has been removed from the page used to submit a certificate request to a superior CA
- 2.4.5.4 Audit trail improvements:
- updated viewer: the user can now filter the events to be displayed by specifying a date range (options: today only, last 7 days, last 30 days, or custom 'from/to' dates)
 - added 'logout due to session time out' event
- 2.4.5.5 Added to the web interface support for the NIST 163-bit Koblitz curve (`us-k-163`); certificate requests submitted to a particular CA account which contain public keys of this type will be accepted (and either queued for review or automatically issued) if '`us-k-163`' is specified as an acceptable key type in that CA's preference settings

2.4.6 Public Site Changes

- 2.4.6.1 The “Suggest Password” feature has been removed from the enrollment pages; use of the NIST FIPS 181 Automated Password Generator on which it was based is now deprecated

2.4.7 CACLI Enhancements

2.4.7.1 Feature and syntax updates:

- added a prompt for the HSM PIN if it is not provided on the command line
- added `-f` option to `-gencrq` to support the output of certificate requests in either binary or PEM-encoded format
- added `-showhash` to display the message digests that can be used with a specified key type/size (following NIST guidelines); if an invalid hash function is specified for key generation, the acceptable hash functions are displayed as part of the error message
- added `-bulkenroll` option to `-addacl` to support the installation of certificates into the ACL for the bulk enrollment interface (BEI ACL) for a specified CA account
- when using `-showacl -ca`, the BEI ACL is displayed along with the web access ACL
- added support for NIST K-163 key generation (`-t` now accepts a `'us-k-163'` argument)
- removed the `-pass` option to specify a self-management password during certificate request submission using `-gensubcrq`

2.4.7.2 Configuration file updates (default-ca-conf.txt and default-subca-conf.txt)

- added `crl.autoIssue.freq` and `crl.autoIssue.freq.unit` to make auto-issuance of CRLs more flexible
- added support for the NIST 163-bit Koblitz curve (`crq.key.ecc=163K`)

2.4.8 New DBAccess Service

- 2.4.8.1 Created an API for the remote execution (via secure RMI) of SQL queries against the CertAgent database; independent DBAccess ACLs are supported on a per-CA basis
- 2.4.8.2 Built a Java library that can be used by authorized clients to pass queries to the DBAccess service; provided sample client code (in Java) to illustrate the use of this library
- 2.4.8.3 Provided a management tool for administrative control of the DBAccess service that can:
- start/stop the service
 - enable/disable and configure the access port for the service on a per-CA basis
 - manage DBAccess ACLs on a per-CA basis

2.4.9 Known Bugs, Limitations, and Workarounds

2.4.9.1 Browser-based Enrollment

- Netscape 4.7 (without Personal security Manager (PSM)): not supported
- Netscape 4.7 (with Personal security Manager (PSM)): when installing a newly issued certificate and chain from the certificate retrieval page, CA certificate(s) are not automatically imported

Workaround: Use the “Install the CA certificate(s) into your certificate store” link to import any missing CA certificates.

- Netscape 7.0: when viewing a newly issued certificate in certificate store, it displays the warning “Could not verify this certificate because the issuer is not trusted.”

Workaround: Select the root CA certificate in the Authorities section of the certificate store. Click Edit and check all the trust settings. Then, click OK to save the changes.

- Mozilla Firefox 1.5: when installing a newly issued certificate and chain from the certificate retrieval page, CA certificate(s) are not automatically imported

Workaround: Use the “Install the CA certificate(s) into your certificate store” link to import any missing CA certificates.

- Internet Explorer on Vista: when installing a newly issued certificate and chain from the certificate retrieval page, the root CA certificate is not automatically imported into CAPI’s “Trusted Root Certificate Authorities” store

Workaround: Download root certificate and manually import it into CAPI’s “Trusted Root Certificate Authorities” store before installing the certificate chain.

2.4.9.2 Renewing Certificates in Internet Explorer on Vista

- Due to a feature change in Microsoft’s CAPICOM library for Vista, ‘renewed’ certificates are not properly associated with existing private keys upon import.

Workaround: At this time the only workaround we can suggest is to not allow certificate renewal or to use a non-Vista system to mediate the update process as follows:

1. on the Vista system, export your old certificate and its private key to a PKCS#12 file
2. move that file to a non-Vista system and import it into Netscape, Firefox, or Internet Explorer
3. open CertAgent’s certificate retrieval page in this same browser and click the link to install your renewed certificate (the non-Vista system will properly associate this certificate with the private key imported from the .p12 file in step 2)
4. export the renewed certificate and its associated private key to a second PKCS#12 file
5. move the second PKCS#12 file back to your Vista system and import it into Internet Explorer

ISC’s Credential Management Utility (CMU) can, of course, be used to automate this procedure to a reasonable degree.

2.4.9.3 Path Validation Issue with Renewed Issuer Certificates

- Browsers (other than Internet Explorer) and other applications that build certificate validation paths by matching the authority key identifier extension in a subject’s certificate with the subject key identifier in the issuer’s certificate may regard as invalid any certificate issued by a CertAgent CA whose certificate has been ‘renewed’ (as their authority key identifier value will have changed). While Internet Explorer does not appear to suffer from this problem, it may be best to avoid using the certificate renewal process for CAs issuing certificates that may be used with other browsers.

2.5 Version 5.0.0

2.5.1 Server Start-Up

- 2.5.1.1 Added ability to specify (`-password`), or prompt for (`-prompt`), the system password when using the command line to start the server

2.5.2 Administrative Site

- 2.5.2.1 Enhanced audit trail
 - categorized events and allowed admin to select one of three logging levels: ‘information and error’, ‘error only’, and ‘off’
 - allowed user to specify which events to log

2.5.3 CA Accounts

- 2.5.3.1 Updated credentials page for newly created CA accounts:
 - allowed selection of existing HSM-based credentials for the new CA account
- 2.5.3.2 Added ability to specify one or more of the following fields in the authority key identifier extension for certificates and CRLs:
 - key ID
 - CA issuer DN
 - issuer serial number
- 2.5.3.3 Enhanced audit trail
 - categorized events and allowed admin to select one of three logging levels: 'information and error', 'error only', and 'off'
 - allowed users to specify which events to log
 - moved bulk enrollment events from request processing to user-initiated actions tab
- 2.5.3.4 Enhanced interactions with external LDAP repositories:
 - added user and CA DN mapping rules to allow certificates to be mapped to the correct entry in the external LDAP repository
 - added option to automatically publish CA certificates to an external LDAP repository
 - if 'publish issued certificates' is enabled, expired, revoked or on-hold certificates will be removed from the external LDAP repository; revalidation of a certificate will cause it to be republished to the LDAP repository
 - if the operation of publishing or removing a certificate from an external LDAP repository fails, it will automatically be retried at midnight; otherwise, the LDAP entries can be updated manually
 - the user and Java keystore passwords required for authenticated LDAP connections are now CMS-encrypted with the system certificate and stored in the configuration file
- 2.5.3.5 Modified configuration settings for the polling of an e-mail server for certificate requests:
 - the e-mail account password is now CMS-encrypted with the system certificate and stored in configuration file
 - the e-mail polling service is now started upon entry of the system PIN/password rather than waiting until the CA server starts
- 2.5.3.6 Added support for contact e-mail address in subject alternative name
- 2.5.3.7 Enhanced 'advanced certificate' page:
 - added option to 'publish certificate to/remove certificate from' an external LDAP repository
 - added option to update a user's contact e-mail address
- 2.5.3.8 Added option to update a user's contact e-mail address to the 'advanced certificate request' page
- 2.5.3.9 Changed default ECC key type to NIST P-256 (from NIST P-192; P-192 is not supported by Microsoft)
- 2.5.3.10 Changed default key sizes for RSA and DSA to 2048 (from 1024)

2.5.4 Public Site

- 2.5.4.1 Updated certificate enrollment via browser page for Vista end-users:
 - CSP drop-down list was replaced with key type list; users can select either RSA or ECC keys
 - Added hash algorithm option
- 2.5.4.2 Added 'Download Root CA' link on certificate retrieval page for Vista users

2.5.5 Key Management Utility

- 2.5.5.1 User is now prompted to save their keystore configuration changes when leaving the ‘manage Java keystore’ page or when exiting the utility
- 2.5.5.2 Detailed results are written to an HTML file instead of appending a simple event log entry to the kmu.log file

2.5.6 Command Line Program

- 2.5.6.1 Updated command line syntax:

new option name	old option name	purpose
genroot	assignroot	generate key pair and assign self-signed certificate to a CA account
gensubcrq	assigncrq	generate key pair; assign certificate request to a CA account and submit to superior CA on same system
gencrq	assigncrq2	generate key pair; assign certificate request to a CA account (for manual submission of certificate request to external CA)
install	replacecrq	install a CA certificate issued by a superior CA on the same machine
installext	replacecrq2	install a CA certificate issued by an external CA
showconf	listconfig	display configuration settings for a CA account or sub-account
showacct	listacct	display all CA accounts, or all sub-accounts of a specified CA account
showslots	listslots	display the slots and labels on an HSM
showkeytypes	listkeytypes	display the types and sizes of keys that can be generated
showacl	listacl	display the ACL for a CA account or sub-account

- o removed [HSM options] when installing a CA certificate
 - o removed ‘-c <country>’ option when creating a new CA account
- 2.5.6.2 Updated the sample configuration files (default-ca-conf.txt, default-subca-conf and cakey-conf-sample.txt) and added some RFC3280 usage guidance.

2.5.7 Bulk Enrollment Interface

- 2.5.7.1 Improved terminology; in particular, replaced ‘pickup’ with ‘retrieve’.

2.5.8 Databases

- 2.5.8.1 Updated the Hypersonic Database library to release 1.8.0.9 (from 1.7.2.4)

2.5.9 Bug Fixes

- 2.5.9.1 If subject alternative name is configured to use the user’s e-mail address and an e-mail address is not provided in the subject DN of the submitted certificate request, the system will issue a certificate without a subject alternative name rather than returning an error
- 2.5.9.2 The status page for a CA sub-account now displays its own e-mail server polling status rather than that of its master account

- 2.5.9.3 The option to export a PKCS#12 file no longer appears on the Export Credential page for HSM-based CA accounts
- 2.5.9.4 Corrected available message digests for ECC keys
- 2.5.9.5 When downloading a PKCS#7 containing CA certificates from the public site, the CA Information page no longer displays duplicate certificates
- 2.5.9.6 If the key size option is not specified, the command line program now defaults to rsa-2048 (rather than to rsa-1024) as suggested by the usage summary

2.5.10 Known Bugs, Limitations, and Workarounds

2.5.10.1 Browser-based enrollment

- Netscape 4.7 (without Personal security Manager (PSM)): not supported
- Netscape 4.7 (with Personal security Manager (PSM)): when installing a newly issued certificate and chain from the certificate retrieval page, CA certificate(s) are not automatically imported

Workaround: Use the “Install the CA certificate(s) into your certificate store” link to import any missing CA certificates.

- Netscape 7.0: when viewing a newly issued certificate in certificate store, it displays the warning “Could not verify this certificate because the issuer is not trusted.”
- Workaround: Select the root CA certificate in the Authorities section of the certificate store. Click Edit and check all the trust settings. Then, click OK to save the changes.
- Mozilla Firefox 1.5: when installing a newly issued certificate and chain from the certificate retrieval page, CA certificate(s) are not automatically imported

Workaround: Use the “Install the CA certificate(s) into your certificate store” link to import any missing CA certificates.

- Internet Explorer on Vista: when installing a newly issued certificate and chain from the certificate retrieval page, the root CA certificate is not automatically imported into CAPI’s “Trusted Root Certificate Authorities” store
- Workaround: Download root certificate and manually import it into CAPI’s “Trusted Root Certificate Authorities” store before installing the certificate chain.

2.6 Version 4.3.0

2.6.1 CA Accounts

- 2.6.1.1 Enhanced searching and reporting for certificate requests:
 - added contact e-mail and last modified date as search criteria
 - allowed user to specify which items to include in the report
 - added sort capability
 - added CSV as a report output format
- 2.6.1.2 Enhanced searching and reporting for issued certificates:
 - added retrieval status and renewal status as search criteria
 - allowed user to specify which items to include in the report
 - added sort capability
 - added CSV as a report output format
- 2.6.1.3 Added a PKCS#12 option to the Export Credential page that allows software-based CA credentials to be backed up to a PKCS#12 file with a specified password

- 2.6.1.4 All base64-encoded certificate links now return PEM-encoded certificates
- 2.6.1.5 Added comment option to Options | Public Site | Enrollment page.
 - if enabled, a comment field will appear on the public enrollment form and any end-user comments will appear on the pending certificate request and advanced certificate request pages
- 2.6.1.6 Changed downloaded PKCS#7 file extension from .p7c to .p7b

2.6.2 Public Site

- 2.6.2.1 Added support for enrollment from Windows Vista
- 2.6.2.2 Added optional comment field to the certificate enrollment page when enabled by the CA
- 2.6.2.3 Changed PKCS#7 download file extension from .p7c to .p7b

2.6.3 Key Management Utility

- 2.6.3.1 Added an option to create temporary administrator, system, and SSL server keys to speed up the initial system configuration process, said certificates to be replaced once the administrator enrolls and certificates with the desired DN and extensions have been issued
- 2.6.3.2 Allowed administrators to view, add, and delete certificate/key entries to/from Java keystores

2.6.4 Certificate Report Generator

- 2.6.4.1 Added retrieval status and renewal status as search criteria
- 2.6.4.2 Added sort capability
- 2.6.4.3 Added CSV as a report output format

2.6.5 Bug Fixes

- 2.6.5.1 If 'check for certificate request duplication' is enabled, a duplicate request is properly detected as soon it is submitted for the second time

2.6.6 Known Bugs, Limitations, and Workarounds

- 2.6.6.1 Browser-based enrollment
 - Netscape 4.7 (without Personal security Manager (PSM)): not supported
 - Netscape 4.7 (with Personal security Manager (PSM)): when installing a newly issued certificate and chain from the certificate retrieval page, CA certificate(s) are not automatically imported

Workaround: Use the "Install the CA certificate(s) into your certificate store" link to import any missing CA certificates.

- Netscape 7.0: when viewing a newly issued certificate in certificate store, it displays the warning "Could not verify this certificate because the issuer is not trusted."
- Workaround: Select the root CA certificate in the Authorities section of the certificate store. Click Edit and check all the trust settings. Then, click OK to save the changes.
- Mozilla Firefox 1.5: when installing a newly issued certificate and chain from the certificate retrieval page, CA certificate(s) are not automatically imported

Workaround: Use the “Install the CA certificate(s) into your certificate store” link to import any missing CA certificates.

- Internet Explorer on Vista: when installing a newly issued certificate and chain from the certificate retrieval page, the root CA certificate is not automatically imported into CAPI’s “Trusted Root Certificate Authorities” store
- Workaround: Download certificates from the CA Information page and manually import them into CAPI’s “Trusted Root Certificate Authorities” store.

2.6.7 Plans for the Next Release

- 2.6.7.1 Allow certificate extensions to be populated based the results of one or more pre-configured LDAP queries
- 2.6.7.2 Add UTF-8 support
- 2.6.7.3 Provide a comprehensive set of configuration parameters for the audit trail, currently configurable only via log4j, on the admin site; administrator will be able to enable or disable logging of all auditable events.

2.7 Version 4.2.0

2.7.1 Administrative Site

- 2.7.1.1 When creating a new CA account, the LDAP search base is no longer limited to a string of the form ‘C=<country>’; the administrator can now specify an arbitrary initial search base that can later be modified by the CA

2.7.2 CA Accounts

- 2.7.2.1 Added CA certificate renewal feature
- 2.7.2.2 Added ECC HSM support
- 2.7.2.3 Added binary and base-64 encoding options when exporting a CA's certificate request
- 2.7.2.4 Modified certificate issuance settings:
 - the following RDN components may be specified:
 - user ID (UID)
 - domain Component (DC)
 - DN qualifier (DNQ)
 - street
 - surname
 - given name
 - initials
 - generation
 - pseudonym
 - the order and number of each of these RDN components can be specified
 - each RDN component can be assigned the property “Require”, “Allow” or “Force”
 - one or more of the following key purpose OIDs may be included in a certificate’s extendedKeyUsage extension:
 - IPSEC End System
 - IPSEC Tunnel
 - IPSEC User
 - IPSEC IKE
 - OCSP Signing
 - Data Validation and Certification Server

- SCVP Responder
- Extensible Authentication Protocol over PPP
- Extensible Authentication Protocol over LAN
- SCVP Server
- SCVP Client

(each of these is represented by a checkbox that can be toggled on or off)

- one or more user-defined OIDs (specified in standard 'dot notation') may be included in a certificate's extendedKeyUsage extension

2.7.2.5 Added a new LDAP | Options page that allows certificates and CRLs to be published to an external LDAP repository

- certificate publishing can be triggered in one of three ways: automatically upon issuance, upon retrieval of the certificate by its subject, or manually
- CRL publishing can be triggered in one of two ways: automatically upon issuance or manually
- displays internal LDAP configuration settings and allows the CA to modify the base for internal LDAP queries

2.7.2.6 Added a new Options | Certificate Management page:

- added an "allow pending revocation" option, which defaults to 'disabled'

If 'disabled', certificates, when initially designated as 'revoked' by a CA, are immediately moved to a 'revoked certificates' list and only those with 'on hold' status can later be reinstated. If this option is 'enabled', certificates, when initially flagged as revoked, are first moved to a list of certificates 'pending revocation' from which they can be reinstated at any time prior to issuance of a CRL (in which they'll appear). Once a CRL containing them has been issued, they are moved to the revoked certificates list from which only 'on hold' certificates can be reinstated.

Motivation: enabling this option allows the CA to change his mind about certificates tagged for revocation and more closely conforms to an X.509/RFC 3280 convention according to which a certificate is not to be considered 'revoked' until it appears on at least one CRL.

2.7.2.7 Modified the Options | Public Site | Enrollment page:

- added default CSP and "enforce" settings
- added an option to disable the self-management password

If 'disabled', a user does not have to specify a password on the certificate enrollment form and is no longer able to submit certificate revocation or renewal requests.

2.7.2.8 Enhanced the audit trail:

- log4j 1.2.14 is now used for all event logging
- a "DailyRollingFileAppender" is used and its event log is scheduled to be rolled over at midnight every day
- administrators can edit the configuration file ('log4j.properties') to simultaneously output log entries to multiple log4j output appenders
- the format of file names has been changed from "MMDDYYYY" to "log.YYYY-MM-DD"

2.7.2.9 Removed UTF-8 support (UTF-8 support will be an option in next release)

2.7.3 Public Site

2.7.3.1 Modified the certificate enrollment page:

- password fields are omitted if the 'self-management' option is disabled by the CA
- default CSP is selected and that may be disabled by CA

- 2.7.3.2 Renamed all “pickup” prompts or menu items to “retrieve” or “retrieval” (simple terminology change)
- 2.7.3.3 Added an “Install the CA certificate(s) into your certificate store” button to the certificate retrieval page for non-IE browsers

2.7.4 Bug Fixes

- 2.7.4.1 Corrected the ordering of RDNs in a subject DN with multiple OUs; the order in the issued certificate will now match the order specified on the CA’s certificate issuance settings page
- 2.7.4.2 The crypto library now produces a correct subject key identifier for ECC root certificates (by SHA-1 hashing the entire ASN.1 DER-encoded public key, rather than just the first part of it)
- 2.7.4.3 Revoking a subordinate certificate with the same serial number as the CA’s certificate now has the correct effect rather than causing subordinate and CA certificates to be revoked
- 2.7.4.4 Viewing the information for a subordinate certificate with the same serial number as the CA’s certificate now correctly displays details of the subordinate certificate rather than those of the CA

2.7.5 Known Bugs, Limitations, and Workarounds

- 2.7.5.1 Enrollment in Windows Vista is not supported but will be in next release
- 2.7.5.2 Browser-based enrollment

- Netscape 4.7 (without Personal security Manager (PSM)): not supported
- Netscape 4.7 (with Personal security Manager (PSM)): when installing a newly issued certificate and chain from the certificate retrieval page, CA certificate(s) are not automatically imported

Workaround: Use the “Install the CA certificate(s) into your certificate store” link to import any missing CA certificates.

- Netscape 7.0: when viewing a newly issued certificate in certificate store, it displays the warning “Could not verify this certificate because the issuer is not trusted.”
- Workaround: Select the root CA certificate in the Authorities section of the certificate store. Click Edit and check all the trust settings. Then, click OK to save the changes.
- Mozilla Firefox 1.5: when installing a newly issued certificate and chain from the certificate retrieval page, CA certificate(s) are not automatically imported

Workaround: Use the “Install the CA certificate(s) into your certificate store” link to import any missing CA certificates.

- 2.7.5.3 SHA-1 is currently the only hash function supported for ECDSA certificate signing with an nCipher HSM. (This is a potential violation of pending 186-3 requirements and is due to bugs in the SHA-2 implementation in the nCipher ECC support library; nCipher has reported that it is working on a solution.)

2.7.6 Plans for the Next Release

- 2.7.6.1 Support certificate enrollment in Windows Vista
- 2.7.6.2 Allow certificate extensions to be populated based the results of on one or more pre-configured LDAP queries
- 2.7.6.3 Add UTF-8 support
- 2.7.6.4 Improve the Key Management Utility:

- Add an option to create temporary administrator, system, and SSL server keys to speed up the initial system configuration process, said certificates to be replaced once the administrator enrolls and certificates with the desired DN and extensions have been issued
 - Allow administrators to add, view, and delete certificate/key entries from the Java keystore
- 2.7.6.5 Provide a comprehensive set of configuration parameters for the audit trail, currently configurable only via log4j, on the admin site; administrator will be able to enable or disable logging of all auditable events.
- 2.7.6.6 PEM-encoding of certificates

2.8 Version 4.1.1

2.8.1 CA Accounts

- 2.8.1.1 Added support for multiple certificate renewal reminders that are to be sent to users on a list of specified days prior to expiration of their certificates

2.8.2 Known Bugs, Limitations, and Workarounds

- 2.8.2.1 Crypto library incorrectly computes the subject key identifier when generating ECC root certificates.

Workaround: do not include subject key identifier or subject key identifier when generating an ECC root certificate.

- 2.8.2.2 Certificate enrollment using browser

- Internet Explorer 5.5: UTF-8 subject and issuer DN's of certificates in the CAPI store do not display correctly
- Netscape 4.7 (without Personal security Manager (PSM)): not supported
- Netscape 4.7 (with Personal security Manager (PSM)): when installing a newly issued certificate and chain from the pick-up page, CA certificate(s) are not automatically imported

Workaround: Use the 'install the CA certificates' link on the CA information page to import any missing CA certificates.

- Netscape 7.0: when viewing a newly issued certificate in certificate store, it displays the warning "Could not verify this certificate because the issuer is not trusted."
- Workaround: Select the root CA certificate in the Authorities section of the certificate store. Click Edit and check all the trust settings. Then, click OK to save the changes.
- Mozilla Firefox 1.5: when installing a newly issued certificate and chain from the pick-up page, CA certificate(s) are not automatically imported

Workaround: Use the 'install the CA certificates' link on the CA information page to import any missing CA certificates.

- 2.8.2.3 When viewing certain pages on the public site using Netscape 4.79, the browser may incorrectly display UTF-8 text fields after scrolling.

Workaround: Select View → Character Set → Unicode (UTF-8) from the menu. Then, select View → Character Set → Set Default Character Set from the menu. Reload the page.

2.9 Version 4.1.0

2.9.1 CA Accounts

- 2.9.1.1 CA credentials:
 - HSM credentials:
 - added message digest options: MD5, SHA1, SHA-224, SHA-256, SHA-384, and SHA-512
 - added 'View Slot/Label' button to display slot and label information for the HSM accessed via the specified library
 - accepts empty PIN if no PIN is required to log in to the HSM
 - software credentials:
 - supports additional message digest options: SHA-224, SHA-256, SHA-384, and SHA-512
 - accepts CA certificates without keyCertSign and/or cRLSign extensions, but if either is missing, the CA will be prohibited from performing the corresponding action
- 2.9.1.2 Certificate issuance settings:
 - added certificate serial number generation option that can be set to 'random' or 'sequence' with specified starting value
 - added message digest options: MD5, SHA1, SHA-224, SHA-256, SHA-384, and SHA-512
 - supports any number of organization units (OU) in the RDN; all OUs' default type must be "Allow", "Required," or "Force"
 - supports serial number in RDN component
 - subject/Issuer alternative name:
 - supports multiple rfc822 names rather than just one rfc822 name
 - supports multiple directory names
 - supports multiple IP addresses
 - authority information access:
 - added OID and URL access method
 - supports subject directory attributes:
 - country of citizenship (US DOD)
 - country of citizenship (RFC 3739)
 - employee type
 - nationality (US DOD)
 - supports Netscape certificate types:
 - SSL client certificate
 - SSL server certificate
 - SSL CA certificate
 - S/MIME user certificate
 - S/MIME CA certificate
 - object signing CA certificate
 - object signing certificate
 - supports qualified certificate statements:
 - id-etsi-qcs-QcLimitValue
 - id-etsi-qcs-QcCompliance
 - NES Telecommunication Agency Authentic Certificate Clause
 - id-etsi-qcs-QcRetentionPeriod
- 2.9.1.3 CRL processing settings:
 - added option to automatically issue a CRL upon certificate revocation / reinstatement; even if this option is enabled, user changes to certificate status on the public site will not trigger CRL issuance
 - added message digest options: MD5, SHA1, SHA-224, SHA-256, SHA-384, and SHA-512
- 2.9.1.4 modified bulk enrollment page to allow posted DN, key usage, citizenship, employee type and subject alternative name values to override their default settings

- 2.9.1.5 advanced certificate request page:
 - added key usage information from the certificate request
 - added submission type information from the certificate request
- 2.9.1.6 certificate search page:
 - added date filter to permit user to specify a range of last modified or expiration dates
 - added 'Export' button to support the saving of search results to a file
- 2.9.1.7 expired certificate page:
 - certificates are now sorted by expiration date (ascending/descending) instead of last modified date
- 2.9.1.8 certificate details page:
 - added binary certificate and binary/base64-encoded PKCS#7 download links
- 2.9.1.9 export credentials page:
 - added binary certificate and PKCS#7 download links
- 2.9.1.10 inspect CRL page:
 - added binary and base64-encoded CRL download links
- 2.9.1.11 added UTF-8 support for input and display to the following fields:
 - certificate/request RDNs
 - other name and DN in issuer/subject alternative name extension
 - NES telecommunication agency authentic certificate clause in QC statement extension
 - user notice in certificate policies extension
 - DN in name constraints extension
 - certificate and request search strings

2.9.2 Public Site

- 2.9.2.1 supports certificate rollover for Internet Explorer users; if user's certificate is about to expire, user can submit a renewal request; during pick-up, renewed certificates are installed into CAPI and associated with their corresponding private keys
- 2.9.2.2 CA information page:
 - added binary certificate and binary PKCS#7 download links for CA certificate
- 2.9.2.3 certificate request upload page:
 - added key usage options: encrypt-only, sign-only, or both
- 2.9.2.4 certificate pick up page:
 - added key backup warning and instructions

2.9.3 Key Management Utility

- 2.9.3.1 added slot and label drop-down list on HSM page to allow HSM self-signed certificate creation with label information
- 2.9.3.2 added Pick Slot/Label button to display slot and label information for the HSM accessed via the specified library
- 2.9.3.3 accepts empty PIN if no PIN is required to log in to the HSM

2.9.4 Command-line Utilities

- 2.9.4.1 added command-line tool to configure CA settings
- 2.9.4.2 added certificate report generation tool

2.9.5 Java Interface

- 2.9.5.1 added bulk enrollment interface to automate certificate enrollment progress via a Java program

2.9.6 LDAP

- 2.9.6.1 supports limiting the size of query results

2.9.7 Known Bugs, Limitations, and Workarounds

- 2.9.7.1 Certificate Issuance page on the CA site: if organizational unit is set to "omit" and saved, a null error is displayed and none of the settings on that page can be changed from that point on. This error is also present on the advanced certificate request page and the certificate enrollment page on the public site.
- 2.9.7.2 When searching for certificates on the public site, entering "*" as a search string results in a database error.
- 2.9.7.3 When attempting to view a certificate in a sub-account's access control list, an "Invalid access" error occurs.
- 2.9.7.4 Certificate enrollment using browser
- Internet Explorer 5.5: UTF-8 subject and issuer DN's of certificates in the CAPI store do not display correctly
 - Netscape 4.7 (without Personal security Manager (PSM)): not supported
 - Netscape 4.7 (with Personal security Manager (PSM)): when installing a newly issued certificate and chain from the pick-up page, CA certificate(s) are not automatically imported

Workaround: Use the 'install the CA certificates' link on the CA information page to import any missing CA certificates.

- Netscape 7.0: when viewing a newly issued certificate in certificate store, it displays the warning "Could not verify this certificate because the issuer is not trusted."
- Workaround: Select the root CA certificate in the Authorities section of the certificate store. Click Edit and check all the trust settings. Then, click OK to save the changes.
- Mozilla Firefox 1.5: when installing a newly issued certificate and chain from the pick-up page, CA certificate(s) are not automatically imported

Workaround: Use the 'install the CA certificates' link on the CA information page to import any missing CA certificates.

- 2.9.7.5 When viewing certain pages on the public site using Netscape 4.79, the browser may incorrectly display UTF-8 text fields after scrolling.

Workaround: Select View → Character Set → Unicode (UTF-8) from the menu. Then, select View → Character Set → Set Default Character Set from the menu. Reload the page.

2.10 Version 4.0.0

2.10.1 Installation

- 2.10.1.1 Introduced a system master key that is used to protect all CA private keys (instead of simply password-protecting them). The system key pair and self-signed certificate can be generated (with a password- or HSM-protected private key) and installed using the integrated Key Management Utility.
- 2.10.1.2 Configuration of the webserver now requires one SSL port with client authentication for the administrative site, and one SSL port without client authentication for the public site.
- 2.10.1.3 The KMU can also be used to generate SSL and HSM key pairs and self-signed certificates.

2.10.2 Administrative Site

- 2.10.2.1 New login URL: `https://<host>:<port>/certagentadmin/admin/login.jsp`
- 2.10.2.2 Account access requires client authentication over HTTPS.
- 2.10.2.3 Administrator manages the access control list of its account and all CA accounts.
- 2.10.2.4 Once the server starts, administrator is responsible for using the Set Password page to enter the system's private key password or HSM PIN.

2.10.3 CA Account Site

- 2.10.3.1 New login URL: `https://< host>:<port>/certagentadmin/ca/login.jsp`
- 2.10.3.2 Account access requires client authentication over HTTPS rather than CA's private key password. Access control list is managed by administrator.
- 2.10.3.3 CA key pair can be generated on an HSM.
- 2.10.3.4 CA private keys are encrypted with the system master key. If a CA's key is stored on an HSM, the HSM PIN is encrypted with the system master key and stored in the configuration file.
- 2.10.3.5 Serial numbers of issued certificates differ from the corresponding request IDs.
- 2.10.3.6 Added "Request ID" search filter on certificate search page.
- 2.10.3.7 Added ability to specify key type and size that system will accept; all other requests are automatically rejected. Master account and sub-account have their own settings.
- 2.10.3.8 Added an option to warn CA and/or user if a certificate request has been previously submitted.
- 2.10.3.9 Added "user" category to audit trail to record user events.
- 2.10.3.10 Added complexity controls to user's self-management password.
- 2.10.3.11 Added lockout mechanism to user's self-management password to thwart exhaustion attacks.
- 2.10.3.12 Added view locked certificate account page to view all the accounts that have been locked.
- 2.10.3.13 Added "unlock account" option in advanced certificate options page.
- 2.10.3.14 Added "send pickup notification to user" option in advanced certificate options page.
- 2.10.3.15 Added two extended key usage options: 'PIV Card Authorization' and 'Microsoft Smart Card Logon'.
- 2.10.3.16 Added support for DNS name, URL, and other name options in issuer alternative name extension.
- 2.10.3.17 Added support for DNS name, URL, and other name options in subject alternative name extension.
- 2.10.3.18 Added authority information access extension.
- 2.10.3.19 Master account now controls the access control lists of sub-accounts.
- 2.10.3.20 Sub-accounts have their own class 1 assurance, email settings, advanced options, and policy settings for certificate issuance rather than sharing such settings with the master account.
- 2.10.3.21 Added an option to allow a sub-account to issue a CRL on behalf of the master account.
- 2.10.3.22 Added an option to allow a sub-account to override the default certificate settings.
- 2.10.3.23 Updated the database structures.
- 2.10.3.24 Display 'assign to' information on certificate and request pages if assigned to filter is set to "anyone".
- 2.10.3.25 Automatic certificate and CRL issuance start after system password/PIN is entered by administrator.

2.10.4 Public Site

- 2.10.4.1 A self-management password is now requested upon submission of a certificate request rather than upon certificate pick up.
- 2.10.4.2 A new self-management password is required with each certificate renewal.
- 2.10.4.3 Added code to allow users to change their self-management password.

