RSA BSAFE® Cert-C 2.7 Release Notes

An RSA Security Engineering Note
March 27, 2003

This note summarizes interoperability targets, significant changes from previous releases, interface behavior issues, and defects in the RSA BSAFE® Cert-C 2.7 software. Please consult the `readme-certc.txt` file, located in the `Cert-C2.7` directory of the CD-ROM media, for information learned immediately prior to product release. Also see the RSA Security Support Web site at www.rsasecurity.com/support/ for the most up-to-date information.

New Features in Cert-C 2.7

The RSA BSAFE® Cert-C 2.7 software release is an incremental update to the RSA BSAFE® Cert-C 2.6 product. The following list summarizes the major new features in Cert-C 2.7:

- Additional messaging objects and APIs for streaming PKCS#7 Data and EnvelopedData. These objects and APIs are documented in `cmsobj.h`. They can be used to stream PKCS #7 message input and output and to minimize memory use. An additional sample has also been provided to demonstrate this functionality.

- Performance enhancements to certificate path building and validation providers, including new APIs in `certlist.h` for adding certificate and CRL objects to LIST_OBJs without the overhead of making deep copies of the added objects.

- Incorporation of RSA BSAFE Crypto-C 6.1 to provide the highest quality cryptographic technology for securing applications.

- The Cryptographic service provider now uses, by default, the full-blinding implementation of the RSA operation to help prevent against timing attacks.

- Sample executables and the rootdb utility are no longer pre-built on the CD-ROM media. If they are desired, you must build them yourself using the provided Microsoft project or Unix/GNU-Linux makefiles. Build the rootdb utility before running the `test.win32` script to batch-execute the samples.

- The setup process for building on the UNIX/GNU-Linux platforms has changed very slightly. Please see the *RSA BSAFE Cert-C Basic Developer's Guide* for the details.

- The Mozilla LDAP client libraries have replaced the iPlanet shared libraries on the HP 11.00 64-bit platform. All platforms now use the Mozilla LDAP client libraries.

New Features in Cert-C 2.6

The RSA BSAFE® Cert-C 2.6 software release is an incremental update to the RSA BSAFE® Cert-C 2.5 product, mainly to support the layering of the RSA BSAFE® SecurXML-C 1.0 toolkit. The following list summarizes the major new features in Cert-C 2.6:

- A new API, `C_SetNameString()`, that sets the contents of a `NAME_OBJ` from the LDAP string representation of a distinguished name. Additionally, sample code is provided that demonstrates its use.

- Cert-C Status Log service provider changes to support multiple format control files for message logging.

- The addition of libraries compiled with multi-thread compiler switches for linking on UNIX and GNU/Linux platforms.

New Features in Cert-C 2.5

The following list summarizes the major new features in Cert-C 2.5:

- PKI messaging redesign—New APIs to manipulate the individual PKI message fields.

- CMP—Additional CMP support to implement certificate revocation, key archival, and key update requesting.

- PKIX—Additional PKIX support to implement CRL distribution points and related extensions in path validation and certificate status checking, and a new algorithm for policy mapping.

- Incorporation of RSA BSAFE Crypto-C 6.0.3 to provide the highest quality cryptographic technology for securing applications.

- The documentation set has been completely redesigned. The reference information is now in HTML format, (the *RSA BSAFE Cert-C Reference*) and there is a new *Basic Developer's Guid*e, as well as the existing *RSA BSAFE Cert-C Developer's Guide*, now called the *RSA BSAFE Cert-C Advanced Developer's Guide*. The *RSA BSAFE Cert-C Service Provider Manual* that shipped with previous releases of Cert-C is now also in HTML format. It is included in the online *Reference*.

- You now have the option to specify single-threaded or multi-threaded code generation with the Microsoft C++ compiler. Cert-C now ships single-threaded and multi-threaded versions of the Cert-C libraries. This is supported only on Win32 platforms.

  For all platforms, Cert-C is threadsafe but not multi-threaded. You can use Cert-C in multi-threaded applications; however, you should not use Cert-C objects in multiple threads at the same time. Doing so might result in corrupted data or other errors. The Cert-C context (which bundles all of the service provider handles) is assumed to be thread-specific.

Interoperability

No changes have been made in Cert-C 2.7 that result in changes to the Interoperability matrix from the Cert-C 2.5 and 2.6 releases.

Cert-C 2.5 has been tested for interoperability with the following vendor products. (This list is not an exhaustive list of possible vendor products that interoperate with Cert-C 2.5.)

Platform OS Support

The following table lists the platforms and operating systems supported by Cert-C 2.7 at the time of release. Ports of the SDK to additional platforms and operating systems are usually available shortly after the release date. Please contact your RSA Security sales or support representative for information on the additional platforms available.

Your RSA Security software contract may not grant you the right to develop applications on all of the platforms listed in the following table. Please contact your RSA Security sales representative for information on the development platforms covered by your contract.

Windows	UNIX
Windows 98 SE	HP-UX 10.20 (PA-RISC 1.1)
Windows NT, Service Pack 6a	HP-UX 11.00 (PA-RISC 2.0, 32 bit and 64 bit)
Windows 2000, Service Pack 3	Solaris 2.6, 8, 9
Windows XP, Service Pack 1	Red Hat Linux 6.2, 7.1, 8.0
	AIX 4.3.3, 5L v5.2

PKI

CMP	
Vendor and Product	**Comments**
Certicom Trustpoint	- CMPv1 & CMPv2.
SSH Certifier 2.1 (pre-release)	- CMPv1 & CMPv2. - Key archival supported.
RSA Keon® Certificate Authority 6.0.2	- Only CMPv2 supported.
Entrust/Authority 6.0	- Only CMPv1 supported. - Server-side key-generation is not supported because Entrust/Authority 6.0 utilizes the proprietary CAST-128 encryption algorithm rather than Triple-DES as required in the CMP Profile specification. - Client-side key archival requests are not supported because the CA public key, which is required to encrypt the EE private key before it is sent to the server, is not published. - EE single-key profile certificate requests (single key is used to sign and encrypt) is not supported. EE separate-keys profile certificate requests (each key has its own key usage) are supported.

CRS	
Vendor and Product	**Comments**
VeriSign OnSite CA	
RSA Keon Certificate Server 5.5	

SCEP	
Vendor and Product	**Comments**
VeriSign OnSite	
RSA Keon Certificate Server 5.x	
RSA Keon Certificate Authority 6.0.2	
Windows 2000 Certificate Authority	- The SCEP server software must be installed from the Windows 2000 Server Resource Kit. - The patch must be applied to the server that is described in "Q272164 MSCEP.DLL Add-on No Longer Functions After One Successful Enroll" located at http://support.microsoft.com/support/kb/articles/q272/1/64.asp. - The CA server software must only be installed in Stand-Alone mode (not in the mode that integrates with Active Directory). - The CA domain under which certificates are issued must be enabled to issue certificates that have pre-shared-secret challenges enabled. In particular, the certificate request process by which a request is made and manual approval is required by the administrator for later retrieval by the client is *not* supported. - The IIS server which front-ends the SCEP requests must be configured to allow requests to be made over http (not https).

Revocation

OCSP	
Vendor and Product	**Comments**
RSA Keon Certificate Authority 5.7	Tested response signing modes: - CA signed responses - Trusted Responder (direct client trust of the OCSP responder) - CA designated responder
RSA Keon Certificate Authority 6.0.2	Tested response signing modes: - CA signed responses - Trusted Responder (direct client trust of the OCSP responder) - CA designated responder (25023) The KCA 6.0.2 OCSP responder does not support DSA signed requests. **Workaround:** Use RSA signed requests. **Releases affected:** 2.0x, 2.5, 2.6, 2.7
ValiCert EVA 4.2.2	Tested response signing modes: - Trusted Responder (direct client trust of the OCSP responder)
VeriSign Onsite CA	Tested response signing modes: - CA designated responder, RSA signed requests and responses

Database

CryptoAPI	
Vendor and Product	**Comments**
RSA Keon Desktop 5.6	RSA Keon Desktop is supported on Windows 98 Second Edition, Windows ME, Windows NT4 Workstation with Service Pack 6a, and Windows 2000 Professional with Service Pack 2.

LDAP	
Vendor and Product	**Comments**
Netscape Directory Server 3.1	

PKCS #11		
Vendor and Product	**Library File**	**Comments**
Gemplus GemSAFE Enterprise Workstation 2.2: - Win32	`pk2priv.dll`	(13467) A crash may occur when using some Gemplus PKCS #11 libraries with certificates having validity dates containing ASN.1 `GeneralizedTime`. **Workaround:** Edit (using `regedit.exe`, for example) the registry key: `HKEY_LOCAL_MACHINE\SOFTWARE\Gemplus\Cryptography\SmartCards\GemSAFE` And change `CertificateCompression` to `"FALSE"`. **Releases affected:** 2.0x, 2.5, 2.6, 2.7
Rainbow iKey 2000: - Win32	`dkck232.dll`	
nCipher nForce: - Win32 - Solaris 2.8	`cknfast.dll` `libcknfast.so`	
Chrysalis Luna 3: - Win32 - Solaris 2.8	`cryst201.dll` `libcrystoki2.so`	

SCEP	
Vendor and Product	**Comments**
VeriSign OnSite	
RSA Keon Certificate Server 5.x	
RSA Keon Certificate Authority 6.0.2	
Windows 2000 Certificate Authority	See notes for PKI SCEP.

Cryptography

CryptoAPI	
Vendor and Product	**Comments**
RSA Keon Desktop 5.6	(8507 and 22010) The Cert-C Default Cryptographic service provider CryptoAPI interface may be unable to determine the correct key size, in bits, of public keys. The provider calls `CryptGetKeyParam()` with `KP_BLOCKLEN` as the value for the *dwParam* parameter, which works with some CSPs such as RSA Keon Desktop 5.1, 5.5, and 5.6, but may not work for other CSPs. **Workaround:** Change the *dwParam* parameter of `CryptGetKeyParam()` to `KP_KEYLEN` in the Cert-C Default Cryptographic service provider `mscrte.c` file and recompile the provider. If the `CryptGetKeyParam()` call fails (no matter what the input parameter is) then the *keyBits* size defaults to `MAX_RSA_MODULUS_BITS`, #defined in `certcryp.h`. **Releases affected:** 1.0x, 2.0x, 2.5

PKCS #11		
Vendor and Product	**Library**	**Comments**
Gemplus GemSAFE Enterprise Workstation 2.2: - Windows NT	`pk2priv.dll`	
Rainbow iKey 2000: - Windows NT	`dkck232.dll`	
nCipher nForce: - Windows NT - Solaris 2.8	`cknfast.dll` `libcknfast.so`	
Chrysalis Luna 3: - Windows NT - Solaris 2.8	`cryst201.dll` `libcrystoki2.so`	

Significant Changes and Bug Fixes from Previous Releases

Significant Change: 31142
Details: `C_GetNameString()` escapes chars with the high bit set.
Result: Change in implementation results in different string output.
Releases affected: 2.6, 2.7

Significant Change: 30411
Details: C_DecodeBase64() should return an error for invalid input
Result: Inputs containing trailing, non-whitepsace text following an otherwise valid base64-encoded string are now rejected.
Releases affected: 2.6, 2.7

Significant Change: 4439
Details: LDAP Database requires use of CodeBase for initialization
Result: The LDAP Database service provider now contains a mechanism to initialize an instance of this service provider using a data structure, rather than data stored in a local RSA/CodeBase database. `S_InitializeLDAP2()` may now be used for this initialization.
Releases affected: 2.5, 2.6, and 2.7

Significant Change: 18071
Details: Relevant revocation information from "obsolete" CRLs was not being used. An obsolete CRL (that is, one whose *nextUpdate* value is earlier than the requested validation time) can still provide useful revocation information, if the certificate in question has been revoked in the CRL (because certificates cannot be unrevoked).
Result: `C_CheckCertRevocation()` will indicate the certificate is revoked `(CERT_REVOCATION.`*`status`*` == CERT_REVOKED)` even if the latest available CRL is obsolete. The only exception to this is if the *reasonCode* indicates "certificateHold", in which case the revocation status will be `CERT_REVOCATION_UNKNOWN` (see current CRL information to see if the certificate has been taken off hold).
Releases affected: 2.5, 2.6, and 2.7

Bug Fix: 33256
Details: C_SelectCRLByIssuerTime() did not return the most recent CRL if CRLs from an issuer were stored across multiple databases. For example, if CRL-1 was stored in the first bound database and a more recent CRL-2 from the same issuer was stored in the second bound database then only CRL-1 was returned, even though there was a better candidate.
Result: All databases referenced by a bound `SERVICE` handle are scanned for candidate CRLs, and the best candidate from the specified issuer is returned.
Releases affected: 2.7

Bug Fix: 33874
Details:. `C_ReadSignedDataMsg()` could not properly parse PKCS#7 signedData message content which was anything but plain PKCS#7 data.
Result: Decoding now works for all types of signed messages, e.g. signed-around-signed-data.
Releases affected: 2.7

Bug Fix: 22163 and 24758
Details: Certificates and CRLs in CryptoAPI stores which could not be parsed by Cert-C (for example, improper use of PrintableString in *IssuerName*) caused certificate and CRL enumeration to fail, preventing any more certificates or CRLs in the store from being retrieved.
Result: Improperly formed certificates and CRLs stored in CryptoAPI are skipped over. A message is logged but no error code is returned.
Releases affected: 2.5, 2.6, and 2.7

Bug Fix: 21717
Details: A certificate issuer's *keyUsage* extension was examined (and usage verified) during path processing only if the extension was marked critical.
Result: The *keyUsage* is verified, regardless of its criticality, when `CERT_PATH_CTX.pathAlgorithm` is `PA_PKIX2`, in accordance with *draft-ietf-pkix-new-part1-12*, section 6.1.4 (n). When the algorithm is `PA_PKIX`, then the *keyUsage* value is verified only if the extension is marked critical, in accordance with RFC 2459 section 6.1 (m). In either case, setting the path processing option `PF_IGNORE_KEY_USAGE` will cause the *keyUsage* extension to be completely ignored.
Releases affected: 2.5, 2.6, and 2.7

Interface Behavior Notes, Known Bugs, and Workarounds

At the time of writing, the following interface behavior issues and known bugs were present in Cert-C 2.7.

Interface Behavior: 4410
Details: It can be difficult to determine the public key type (RSA or DSA) in a certificate. The public key type is necessary to set `SIGNER_INFO.signatureAlgorithmId` value when sending signed messages.
Workaround: Use Crypto-C's `B_DecodeAlgorithmBER()` API to examine a certificate object's `CERT_FIELDS.publicKey` value. If the returned `algFlag` value is `BSAFE_KI_DSAPublicBER`, `BSAFE_KI_DSAPrivateBER`, `BSAFE_KI_DSAPublicX957BER`, or `BSAFE_KI_DSAPrivateX957BER` then the key is a DSA key. It is an RSA key if the returned value is `BSAFE_AI_PKCS_RSAPubOrPrivateBER` or `BSAFE_KI_RSAPublicBER`.
Releases affected: 2.7

Interface Behavior: 25114
Details: `C_ReadSignedDataMsg()` adds all signers to either the `unverifiedSigners` list parameter or the `verifiedSigners` list parameter. If a signer's signature is verified and the signer is validated, the signer is added to the `verifiedSigners` list; otherwise, the signer is added to the `unverifiedSigners` list. (Verifying a signer's signature means the signer's certificate is found, and the calculated message digest matches the signed digest. Validating the signer means the certificate is not expired and a valid path is found according to the specified path context.)
Workaround: None.
Releases affected: All

Interface Behavior: 25311
Details: Even though the Cert-C 2.5 PKI APIs allow creation of multiple messages in a PKI message, such messages have not been verified with any of the providers.
Workaround: Send only single messages in a PKI message.
Releases affected: 2.5, 2.6, and 2.7

Interface Behavior: 14561
Details: CodeBase databases cannot be used on NFS filesystems. The Cert-C Default Database service provider uses CodeBase as its database engine. The CodeBase code as compiled for Cert-C does not operate correctly when databases are created or used on NFS.
Workaround: Databases must reside on local filesystems.
Releases affected: All

Interface Behavior: 17972
Details: Correspondence between a private key being inserted into a database and the accompanying certificate or SPKI is not verified, for example, by performing a sign-verify operation on dummy data.
Workaround: If necessary, the application can verify that the private key corresponds to the given certificate or SPKI prior to the insert operation.
Releases affected: All

Bug: 31311
Details: `C_SetNameString()` incorrectly encodes OID values (when used instead of one of the well-known attribute types) if any of the node values are > 2^32.
Workaround: Do not use these OID values. These OID values are virtually non-existent.
Releases affected: 2.6, 2.7

Bug: 18136
Details: `C_SetCertBER()` rejects certificate BER encodings containing critical extensions unknown to the toolkit.
Workaround: There are two separate workarounds:
1. Make sure unknown extensions are not critical, or
2. Register an extension handler for the desired extension before setting cert objects with the BER encoding.
Releases affected: All

Bug: 4507
Details: In `C_ValidateCert()`, if you attempt to validate a `CERT_OBJ` that was created using the old BCERT-style call, with `(APPL_CTX)NULL_PTR` as the second parameter, `C_ValidateCert()` will crash on Win32.
Workaround: Do not mix old style BCERT and new style Cert-C calls in an application. See appendix B, in the *RSA BSAFE Cert-C Basic Developer's Guide*, for more information about compatibility issues to consider when migrating BCERT

applications to Cert-C.
Releases affected: All

Bug: 4619
Details: Cert-C returns `E_DATA` to the application when parsing a BER-encoded certificate with a validity date exceeding December 31, 2099.
Workaround: None.
Releases affected: All

Bug: 25776
Details: If an application specifies `LDAP_DATA.sizeLimit` to be zero, the expected behavior is, there is no limit to the number of certificates that a search can return. However, the Cert-C LDAP Database service provider currently forces `LDAP_DATA.sizeLimit` to be `DEFAULT_LDAP_SIZE_LIMIT`, when `ldap_set_option(LDAP_OPT_SIZELIMIT)` is called. `DEFAULT_LDAP_SIZE_LIMIT` sets a limit of 200 certificates, as established in `provider/db/ldap/ldapprv.h`. So, if `LDAP_DATA.sizeLimit` is set to zero, then the search can return up to 200 certificates. If the result of the search is more than 200 certificates, then an `E_LDAP_ERROR` (0x770) is returned. It is probable that this service provider will be changed in a future patch or release to pass-through the user-set value of `LDAP_DATA.sizeLimit`.
Workaround: Specify a sufficiently large, non-zero value for `LDAP_DATA.sizeLimit`
Releases affected: All

Documentation Issues

RSA BSAFE Cert-C Reference

When the online *Reference* is viewed with the Netscape browser, resizing the window may cause the left frame, which contains the table of contents, to disappear. If this occurs, reload `certc_reference.html`.

The RSA Security Web Site

The RSA Security Web site, www.rsasecurity.com, has Web pages for Cert-C product information (www.rsasecurity.com/products/bsafe/certc.html). The RSA Laboratories Web site, www.rsasecurity.com/rsalabs/, has pages for security bulletins, coming events, and FTP. RSA Laboratories' Cryptography FAQ is available at www.rsasecurity.com/rsalabs/faq/.

Third-Party Licenses

This product may include software developed by parties other than RSA Security. The text of the license agreements applicable to third party software in this product may be viewed in the `thirdpartylicense.pdf` file. All other code in the RSA BSAFE Cert-C product is covered by the RSA Security software license agreement.

Getting Support and Service

RSA Security is committed to helping you effectively integrate our security components into your applications. Bug reports, comments, and other suggestions are welcome via e-mail to `bugs@rsasecurity.com`. You can get technical support as follows:

General Support Information

General support information is available online at www.rsasecurity.com/support/.

SecurCare® Online

You may open cases through SecurCare. For more information about SecurCare, please visit our Web site at www.rsasecurity.com/securcare/index.html.

Trademarks