

BCERT™ Toolkit

RSA's Certificate Issuing and Key Management Toolkit for Developers

Today's secure communications rely on public key technology, and in this environment, the authenticity of an RSA public key is crucial. Without solid assurance that an RSA public key belongs to the person or organization it represents, one might unknowingly transmit secret information directly into the hands of an imposter or spy — or accept that imposter's digital signature as authorization for a critical electronic business transaction.

The Answer: The "Digital ID"

A digital certificate is essentially a "digital ID" that notarizes the connection between an RSA public key and its legitimate owner — just like a driver's license proves your identity in the physical world. And just as you wouldn't go anywhere without your driver's license, users of secure networks rely on digital certificates to vouch for their digital identity.

The CCITT X.509 Digital Certificate is the internationally recognized electronic document used to prove identity and public key ownership over a communications network. Each certificate contains the issuer's name, the user's public key and identifying information, and the issuer's RSA digital signature. This signature, which validates the certificate, also "seals" the certificate so that it can't be forged or altered.



Introducing BCERT

Until now, building certificate management engines was a difficult — and often risky — chore for the secure applications developer. X.509 certificate management and the issues associated with "digital notarization" made certificate issuing a challenging undertaking, for even the most experienced product development team. But RSA's new BCERT toolkit makes it easy. With BCERT, you can add full-functioned certificate issuing to just about any RSA-secured application — quickly, easily, and with confidence.

BCERT provides full support for CCITT X.509 v3 certificate extensions — and even provides utilities that allow your applications to create their own certificate extension types and incorporate them into BCERT's own extensions-processing engine.

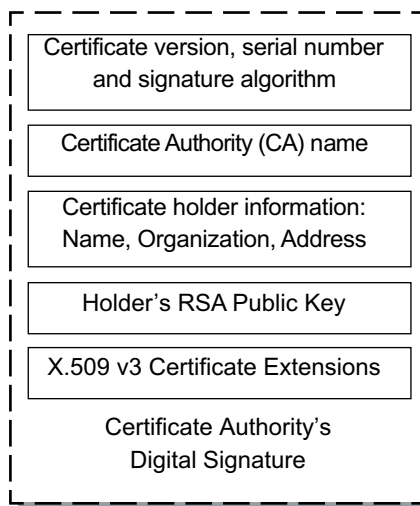


Diagram of an X.509 Certificate

Use the Most Trusted CA's

BCERT contains all the cryptographic support necessary to generate certificate requests, sign certificates and create and distribute certificate revocation lists (CRLs). BCERT also easily interfaces with existing commercial certification services, such as those available from VeriSign, the US Postal Service, and others. Or, if you so desire, you can strike out on your own, and define your own enterprise certification hierarchies, root keys, and notarization policies. With BCERT, it's totally up to you.

Building on BSAFE

The BCERT toolkit is built on top of the most trusted cryptography engine in the world — RSA's own BSAFE toolkit — and like BSAFE, BCERT features an object-oriented API utilizing data abstraction for more efficient development. BCERT is also re-entrant, so it can be shared by many applications at the same time — a necessity in today's multitasking operating environments. Long, computationally-intensive cryptographic operations are interruptible or even cancelable, and there are a variety of platform-specific optimizations available.

How to Get BCERT

To purchase a copy of the BCERT toolkit, or if you would like more information on any of our products, please call an RSA representative at (415) 595-8782.

BCERT™ 1.0 Specifications

Features

- General purpose, low-level certificate formatting and parsing engine for software developers
- Creates certificate requests that can be fulfilled by Verisign and other commercial certification services
- Portable C API, source licensing available
- Fully supports X.509 certificates (v1, v2 and v3)
- Supports standard X.509 version 3 certificate extensions:
 - Authority Key Identifier
 - Subject Key Identifier
 - Certificate Policies
 - Basic Constraints
 - Key Usage Restriction
 - Issuer Alternative Name
 - Subject Alternative Name
 - Subject Directory Attribute
 - Policy Constraints
 - Private Key Usage Period
- Accepts user-defined extension types and adapts to unknown extension types
- Supports PKCS #10 certificate requests with X.509 v3 certificate extensions
- Supports Certificate Revocation Lists (v1, v2)
- Supports X.509 v3 CRL extensions:
 - Authority Key Identifier
 - CRL Number
 - Delta CRL
 - Issuer Alternative Name
 - Reason Code
 - Instruction Code
 - Invalid Date
- Suitable for real-time authentication applications.
- Supports the following RSA digital signature algorithms:
 - MD2 with RSA encryption
 - MD5 with RSA encryption
 - SHA1 with RSA encryption
- Re-entrant: supports multiple threads of execution
- Supports customization of the supported standard extensions
- Supports user-definable key sizes up to 2048 bits
- Supports ASN.1 BER and DER encoding

Potential BCERT 1.0 Applications

Developers can use BCERT as a certificate engine for many different types of certificate issuing applications including:

- Certificate authorization and issuing centers
- Internet electronic commerce and electronic payment systems
- Secure software distribution and copyright protection
- Secure World Wide Web applications
- Non-repudiable digital signatures for electronic records, contracts, and files

System Requirements

Platforms:

- Windows 3.1, Win95, and Windows NT
- UNIX
- Macintosh
- Others (Contact RSA)

Memory:

- Flexible, varies by application

Related RSA Product Offerings

Developers wishing to add cryptography to their applications should consider BSAFE 3.0, RSA's general purpose modular cryptographer's toolkit.

Users requiring both signature and encryption capabilities for electronic messaging should examine TIPEM 2.0, RSA's toolkit for full-featured privacy and authentication applications.

Also available from RSA is RSA Secure, a fast and reliable file security application for data encryption on your desktop or laptop. RSA Secure is available for both Windows and Macintosh users.

BCERT Pricing

See a current RSA pricing information sheet for developer pricing. Volume discounts, site licensing and distribution pricing are also available. Contact RSA for details.

Contacting RSA



RSA Data Security, Inc.
100 Marine Pkwy Ste. 500
Redwood City, CA 94065
Phone: 415-595-8782
Facsimile: 415-595-1873
info@rsa.com
<http://www.rsa.com/>

RSA products contain proprietary, confidential, and/or trade secret RSA encryption algorithms and subroutines. Applications developed with RSA products, if distributed or sold, are subject to additional licensing. Source code licensing is also available. Contact RSA for details.

Copyright © 1996 RSA Data Security, Inc.
All rights reserved. The RSA Public Key Cryptosystem is protected under U.S. Patent # 4,405,829.