



The Security Division of EMC

RSA Solution Brief

RSA BSAFE®

Security Tools for Java Developers

Introduction

Built on more than 20 years of expertise in delivering high-quality products for implementing strong security controls in software and networked applications, RSA BSAFE® security software for Java developers:

- Combines the core security functionality into one common, interoperable and flexible set of libraries
- Provides solutions which support the latest industry standards, as well as industry and government requirements, like FIPS 140
- Provides a 100% Pure Java™ implementation that supports the Java Cryptography Extensions (JCE) standard interface
- Provides strong, reliable data encryption for commercial and government use
- Offers proven components that speed time to market for your solutions

JAVA DEVELOPER SECURITY REQUIREMENTS	RSA BSAFE® SOLUTIONS
100% Pure Java implementation	RSA BSAFE software tools are a 100% Pure Java™ implementation giving Java developers the interoperability and portability they expect from Java components.
Support for Java security development standards	RSA BSAFE software for Java developers includes a provider that complies with the Java Cryptography Extensions (JCE) standard enabling developers to use familiar interfaces to add security to their applications.
FIPS 140 Support	RSA BSAFE software is one of the few FIPS 140-validated, Pure Java™ implementations available on the market. This is essential for developers needing to offer their applications to U.S. Federal Government clients. FIPS 140 support is available through both the JCE and proprietary provider modules.
Obfuscation Support	Supports obfuscation of sensitive data when not in use and bytecode obfuscation to prevent unauthorized use of protected methods and classes.
Compliance with Public Key Cryptography Standards (PKCS)	RSA BSAFE software complies with Public Key Cryptography Standards (PKCS) which define cryptographic processes for easy interoperability. Adherence to these standards, such as PKCS #7, ensures compliance with customer privacy and regulatory requirements, allows the signing of data messages and the opening of enveloped messages in the processing of large data blocks.
High Performance Even for Complex Processes	RSA BSAFE software has memory management and protection services to allow more control of the memory allocated to hold the output of large math calculations, which ensures high performance. Developers also have the option of using C/C++ Native code services to further optimize performance for their Java applications.
Support for X.509 Certificates	RSA BSAFE software supports requesting, creating and parsing X.509 certificates. This provides interoperability with X.509 digital certificates issued by standards-based certificate authorities.



Companies are becoming more wary of acquiring software that does not meet the security requirements they are establishing. Most software developers think they can get all the security they need by default from the Java™ platform. While the Java platform provides good baseline security capabilities, many commercial software applications require security functionality beyond that provided by the Java platform. RSA BSAFE® security tools for Java developers provides a complete set of common libraries written in pure Java for meeting the core security requirements of commercial software applications.

RSA BSAFE software helps Java application developers meet these customer requirements. The software also extends the core security capabilities of the Java platform by meeting the stringent FIPS 140 requirements, the U.S. government standard which specifies the security requirements to be satisfied by a cryptographic module to be used by a Federal agency. The security components provided by the Java platform do not have this support — using only the baseline support can greatly increase your time-to-market as you will need to go through the FIPS 140 validation process yourself. Our Java software with FIPS 140 validated cryptographic modules save you from this time and resource-intensive effort.

Support for standards such as FIPS 140 highlights RSA's commitment to providing strong, effective, and up-to-date solutions for our customers designed to meet the strictest requirements. Thousands of commercial software applications from respected companies such as Adobe, Microsoft, and Computer Associates rely on RSA BSAFE tools in their own products. Our over 20 years of experience in delivering high-quality security tools helps ensure working with RSA will keep security from becoming an unnecessary burden on your project.

Cryptographic Components for Java Programmers

Companies are putting more and more pressure on software developers to employ strong security techniques such as encryption to ensure the privacy of sensitive data as well as close vulnerabilities in their applications. Additionally, data security must be

Java Software for Meeting Evolving Security Requirements

persistent for the life of a transaction, from the point of execution through to fulfillment and reconciliation. Implementing RSA BSAFE Crypto software's strong encryption technology helps developers build trust into applications which can then provide persistent protection for sensitive data.

Non-repudiation and Strong Authentication

Establishing trust in a transactional environment requires certification of the integrity of individual transactions. Trust must also “persist” throughout the life of the transaction. Two major components are required: validation the transaction comes from an authorized sender, and only that sender, and certification the transaction contents remain unchanged. RSA BSAFE Cert software enables Java developers to integrate digital transaction signing capabilities which provide a “seal of approval” on the sender's identity as well as a secure digital “wrapper” around the contents. This helps enforce non-repudiation because applications have a record of exactly when and by which entity the transaction was initiated. These capabilities help establish a network of trust for your electronic transactions.

Data Security over Open Networks

The Sarbanes-Oxley Act and other regulations require companies to establish greater control over sensitive information. Effective security requires “defense in depth”—multiple layers of control. Most companies have deployed firewalls and proxies to secure externally traveling transactions, but ensuring persistent security inside the network is also required. RSA BSAFE SSL software helps developers provide protection for transactions as they travel between applications, ensuring the network link between the application and the next intended destination is a trusted link—safe from prying eyes.



RSA BSAFE Crypto: Strong Encryption Technology for Software Developers

At a Glance

- Helps application developers comply with data privacy regulations
- Persistent protection for application data at rest without compromising existing data models
- High-performance implementations offer effective security without compromising application demands
- Support for open industry standards ensures interoperability with existing infrastructure and flexibility to adapt to regulatory changes over time
- Proven components from an industry leader means faster time to market

Persistent Protection for Data at Rest

Persistent protection requires you to properly secure sensitive data at rest in back-office database systems in addition to standard network security controls. Our RSA BSAFE Crypto software is designed to help you protect sensitive data as it is stored using strong encryption techniques that ease integration with existing data models. RSA BSAFE Crypto software also supports a wide range of industry standard encryption algorithms offering you the flexibility to choose the option most appropriate to your requirements. The software also incorporates performance optimizations to ensure security does not become a bottleneck to the throughput requirements of your applications. Using the capabilities of RSA BSAFE Crypto software in your application will help provide a persistent level of protection for data, lessening the risk of internal, as well as external, compromise.

Standards Support Eases Integration Into Your Environment

Another reason RSA BSAFE Crypto software is used so widely is the software is designed to support many global security standards so important to the business, financial and electronic commerce networks around the globe. RSA also submits its cryptography software for rigorous FIPS 140 testing and validation, the U.S. government standard which specifies the security requirements to be satisfied by a cryptographic module to be used by a Federal agency. This certification further highlights RSA's commitment to providing strong, effective, and up-to-date encryption solutions for our customers.

Key Features of RSA BSAFE Crypto

- A broad range of asymmetric (public key) algorithms, symmetric (secret key) ciphers and message digests provides flexibility for a wide variety of security needs.
- Random number generation via FIPS 186-2-based PRNG, HMAC Deterministic Random Bit Generator (NIST SP 800-90), Dual Elliptic Curve Deterministic Random Bit Generator (NIST SP 800-90), MD5-based PRNG, and SHA-1-based PRNG.
- Key generation services automate key generation and provide for the creation of cryptographic keys.
- Cryptographic syntax and data encoding services comply with public key cryptography standards (PKCS) for more seamless interoperability.
- Memory management and protection services provide more control of the memory allocated to hold the output of large calculations, providing more flexibility.

Persistent protection requires you to properly secure sensitive data at rest in back-office database systems in addition to standard network security controls.



RSA BSAFE Crypto Features

Standards Support	FIPS 140-2 Validated Crypto Module
	ANSI X9.31 Support
	PKCS #1, #5, #8, #11 and 12 Standards Support
Cryptographic Services	Cryptographic Multi-Precision (CMP) Library
	Message Digests
	Symmetric Algorithms
	Asymmetric Algorithms
	Random Number Generation
Application Services	Padding Selection
	Advanced Key Seeding Routines
	Key Generation
Platform Services	Java Cryptographic Extensions (JCE) Provider
	Obfuscation
	Native Code Services (via JNI)
	Threading
	Time
	PKCS #11 Interface

- High-speed math processing provides great performance in calculations of large numbers — especially critical in public key operations — saving valuable time.
- Native code services provide the ability to use native C code for improved performance.
- Memory obfuscation to protect sensitive data when not in use and byte code obfuscation to prevent the unauthorized use of sensitive methods and classes.

RSA BSAFE Cert: Non-repudiation and Strong Authentication for Sensitive Transactions

At a Glance

- Helps establish a network of trust for electronic transactions
- Allows developers to validate digital signatures to certify the integrity of transactions
- Supports non-repudiation by offering certification of a sender's identity for a transaction
- Support for open industry standards ensures interoperability with existing infrastructure and flexibility to adapt to regulatory changes over time
- Proven components from an industry leader means faster time to market

Public Key Infrastructure: The Open Standard for Establishing Integrity

The security demands on today's software applications are rapidly changing. The growth of business process automation and business-to-business integration using the Internet requires a mechanism for digital trust not accomplished by traditional physical barriers, usernames/passwords and other authentication and verification methods. Public key infrastructure (PKI) leverages public key cryptography and provides a unified, scalable framework for securing a wide range of enterprise and Internet applications. The scalability of PKI comes from the use of public/private key pairs and the comparative safety in exchanging public keys over open networks. PKI-based digital certificates allow developers to bind public keys to the identities of individuals and entities—to support authentication, credential validation and the establishment of rules of trust between parties in a transaction. RSA BSAFE Cert software provides the capabilities software developers need to implement this open standard into their transactional environment.

Simplifying Development and Deployment of a Network of Trust

RSA BSAFE Cert software gives application developers the capabilities they need to simplify the development of applications for managing digital certificates and integration into a public key infrastructure. These products help organizations and software vendors build open PKI applications and security products not tied to a single PKI vendor. Applications created with these products seamlessly and automatically interoperate with existing PKI products that support Public Key Cryptography Standards (PKCS) and Public Key Infrastructure x.509 (PKIX) standards. In addition to the certificate management functionality, RSA BSAFE Cert software includes protocol support for real-time PKI interaction, including certificate request/response operations such as certificate enrollment, look-up and validation.

Key Features

- Directory and PKI access services provide flexibility, interoperability and developer ease of use through a directory interface which provides storage and retrieval of keys and certificates. PKI access allows for certificate-enabled applications to work out of the box with standards-based certificate authorities.
- Cryptographic message syntax (CMS) services support standards on how to encode signed and/or enveloped messages so they may be securely exchanged over open networks to allow for interoperability and ease of use.
- Trust services allow increased flexibility by supporting chain validation of hierarchical trust relationships and support for multiple trust models, e.g., self-signed certificates and explicit trust relationships.
- Certificate services provide facilities to create, request, retrieve and store digital certificates, including support for self-signed certificates and qualified certificates. Support for certificate extension extraction and certificate revocation enables full certificate life-cycle management.
- Key handling services support generating public/private key pairs, extracting public keys, and importing and exporting of keys.

RSA BSAFE Cert helps simplify the development of applications for managing digital certificates and integration into a public key infrastructure.

- Key, certificate and trust secure stores provide an online certificate status protocol (OCSP) certificate server to provide access to status information as well as support for client-side private key/certificate storage using a full-featured database, LDAP directory or file system.
- Digital signature services support signing data and verifying signatures with PKCS#7 signatures or digital signatures via cryptography product.
- RSA BSAFE Cert software is built on the strong cryptographic and authentication services provided by RSA BSAFE® Crypto software.
- Request a certificate via PKCS#10, public key cryptography infrastructure (X.509) [PKIX], Certificate Request Syntax (CRS) or Certificate Management Protocol (CMP).
- Retrieve a certificate via PKCS#7, Basic Encoding Rules (BER), Distinguished Encoding Rules (DER), CRS or CMP.
- Process a certificate:
 - Extract a public key
 - Generate a self-signed certificate
 - Extract certificate extensions (parsing)
 - Provide for full certificate extension support
 - Verify a certificate signature
- Revoke a certificate with CMP.
- Check a certificate revocation with Online Certificate Status Protocol (OCSP) and Certificate Revocation List (CRL).

RSA BSAFE Cert Features

Trust Services	Multiple Trust Model Support: Hierarchical and Explicit
	Chain Validation
	Online Certificate Status Protocol (OCSP) Support
	Certificate Revocation List (CRL) Support
Certificate Services	Cryptographic Message Syntax (CMS) Services
	Certificate Lifecycle Management — Request, Retrieve, Process and Revoke Certificates
	Generate Self-Signed Certificates
	Import and Export Keys or Certificates
	Java Certification Path (JCP) Provider
Directory and Storage Services	Interoperability with X.509 v3 Standards-Based CAs
	Private Key and Certificate Storage
Cryptographic Services	FIPS 140 Validated Cryptographic Module
	Message Digests
	Asymmetric Algorithms
	Key Generation
Platform Services	PKCS#11 Interface
	Threading
	Time
	Obfuscation
	Native Code Services (via JNI)

- Import keys and certificates from other sources with PKCS #7, 8 and 12.
- Export certificates to other sources with PKCS #12.
- Export private keys to other sources with PKCS #8.

RSA BSAFE SSL: Protection for Sensitive Data Traveling over Open Networks

At a Glance

- Provides protection for sensitive data as it travels over open networks, both internal and external
- Uses the open standard Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols to provide data protection for network transactions
- Allows developers to implement persistent protection for sensitive transactions to the edge of the network
- Proven components from an industry leader means faster time to market compared to open-source offerings

Secure Sockets Layer (SSL): The Open Standard for Creating Trusted Networks

Secure Sockets Layer (SSL) is the Internet security protocol for point-to-point connections. It provides protection against eavesdropping, tampering and forgery. Clients and servers establish a secure link (or “pipe”) across the Internet to protect the information being sent and received. Customers can have confidence their information is confidential, authentic and original during an Internet connection using SSL. It is a formidable task for developers to become familiar with the various areas to consider, such as: the protocol infrastructure, upper layer services and underlying cryptographic algorithms. Using RSA BSAFE software, developers can easily add support for creating trusted network links between applications providing persistent security for transactions as they travel over open internal and external networks.

Extending Security to the Edge of the Network

The tools of electronic transactions and the technologies that support them—from the Internet and e-mail to VPN and WAP gateways—all are vulnerable to attack by hackers and mischief-makers. These transactions and agreements can be tampered with, forged and blocked, while communications sent via e-mail and wireless technologies can be intercepted and their confidentiality broken. These threats also extend inside the network perimeter. Regulatory compliance

and assurance of data privacy requires persistent enforcement of security rules throughout the network. RSA BSAFE SSL software will help application developers build persistent enforcement into their applications for all network transactions from the edge of the network through to internal systems.

Key Features

- Support for standard SSL v3, TLS v1.0, TLS v1.1 and TLS v1.2 protocols.
- Support for public key cryptography standards (PKCS) #1, 7, 8, 10, 11 and 12.
- Supports requesting, creating and parsing X.509 standard digital certificates.
- Supports client / server authentication and message authentication using the HMAC standard.
- Network layer optimizations support multiple network protocols with a built-in protocol handler and session caching.
- Improves scalability by including code optimizations to run on popular platforms and processors as well as supports multi-threaded use. RSA’s implementation of HP’s patented MultiPrime™ technology helps optimize the performance of RSA private key operations in SSL transactions.

SSL is the Internet security protocol for point-to-point connections. It provides protection against eavesdropping, tampering and forgery.

RSA BSAFE SSL Features

Protocol Services	Network Layer Optimizations
	Blocking I/O Support
	Session Caching
	Built-in Protocol Handler
	TLS v1.0, v1.1, and v1.2 Support
	SSL v3 Support
Certificate Services	PKCS #1, #7, #8, #10, #11 and #12 Support
	Client and Server Authentication Services
	Certificate Management Services
Cryptographic Services	FIPS 140 Crypto Support
	Protocol Cipher Suites
Platform Services	Obfuscation
	Native Code Services (via JNI)
	PKCS #11 Interface

Appendices

Complying with Data Security Guidelines for Government Systems

Our technology meets or exceeds the information security best practices and requirements established by the U.S. National Institute for Standards in Technology (NIST) and the U.S. National Security Agency (NSA) as specified in FIPS 140 and other security standards. Our customers including Lockheed Martin, Northrop Grumman, the U.S. Department of Homeland Security, the U.S. Senate, and many other agencies and their suppliers count on RSA technology that meets these standards to keep highly sensitive information protected.

RSA submits its cryptography products for FIPS 140 testing and validation through the rigorous Cryptographic Module Validation Program (CMVP) established by NIST. The FIPS 140 validation program assures cryptographic libraries meet defined characteristics for robustness, security of the architecture, and support for standard algorithms. We continually update our solutions to meet the latest NIST guidelines so our customers have the confidence of using the most reliable security technology available for protecting network transactions, data stores, and device applications.

PLATFORM SUPPORT	CRYPTO	CERT	SSL
Microsoft® Windows®	✓	✓	✓
Sun® Solaris™	✓	✓	✓
HP-UX	✓	✓	✓
Red Hat® Linux®	✓	✓	✓
IBM® AIX®	✓	✓	✓
z/OS	✓		
OS/400	✓		
Confirmed interoperability testing for “ports” on other platforms available	✓	✓	✓

Platform Support

- 100% Pure Java technology
- Supported JDKs — Sun, HP and IBM

Algorithm Support for Crypto, Cert and SSL Software

- RSA, RSA with MultiPrime™ technology, DSA and Diffie-Hellman
- AES, RC5®*, RC4®, RC2®, DES, 3DES and DESX**
- MD2, MD5, HMAC, SHA-1, SHA-224**, SHA-256*, SHA-384*, SHA-512*, RIPEMD-160**, HMAC-MD5, HMAC-SHA1, HMAC-SHA224**, HMAC-SHA256*, HMAC-SHA384*, HMAC-SHA512*, HMAC-RIPEMD-160**
- Elliptic Curve Digital Signature Algorithm (ECDSA)**
- Elliptic Curve Diffie-Hellman (ECDH)**
- ECDH with co-factor (ECDHC)**
- Elliptic Curve Authenticated Encryption Scheme (ECAES)**
- Elliptic Curve Integrated Encryption Scheme (ECIES)**

Supported Standards

- FIPS 140 validated cryptography for use by Crypto, Cert, and SSL products
- Protocol Support: SSL v3, TLS v1.0, TLS v1.1, and TLS v1.2
- American National Standards Institute (ANSI) — X9.31 — for Crypto
- Public Key Cryptography Standards (PKCS) #1, 5, 8, 11, and 12 — for Crypto
#1, 3, 5, 7, 8, 10, 11 and 12 — for Cert
#1, 7, 8, 10, 11, and 12 — for SSL
- Certificate format — X.509 v3 — for Cert and SSL
- LDAP directory — v2 — for Cert
- Random Number Generation - FIPS 186-2 based PRNG, HMAC Deterministic Random Bit Generator (NIST SP 800-90), Dual Elliptic Curve Deterministic Random Bit Generator (NIST SP 800-90), MD5-based PRNG, and SHA-1-based PRNG
- Certificate Status Methods — X.509 CRLs and OCSP

* Supported in the RSA BSAFE Crypto and Cert software

** Supported only in the RSA BSAFE Crypto software



RSA is your trusted partner

RSA, The Security Division of EMC, is the expert in information-centric security, enabling the protection of information throughout its lifecycle. RSA enables customers to cost-effectively secure critical information assets and online identities wherever they live and at every step of the way, and manage security information and events to ease the burden of compliance.

RSA offers industry-leading solutions in identity assurance & access control, encryption & key management, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.

©2007-2009 RSA Security Inc. All Rights Reserved.
RSA, RSA Security, SecurID and the RSA logo are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. Windows and Microsoft are registered trademarks or trademarks of the Microsoft Corporation in the U.S. and/or other countries. EMC is a registered trademark of EMC Corporation. All other products and services mentioned are trademarks of their respective companies.

BJD SB 1009



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC