



RSA BSAFE® Data Security Manager

Simplifying development and deployment of secure applications

New regulatory pressures and demands from customers and partners to better protect sensitive information are elevating the importance of designing for security as well as for functionality. Improperly secured applications greatly increase the risk of exposure or breach. Most companies cannot afford both the loss to their business and to their reputation which results from such a breach. Security needs are becoming just as important as functional needs in order to successfully mitigate business risk. How do companies avoid data security vulnerabilities without greatly increasing the cost of developing and deploying new business applications?

AT A GLANCE

- Provides easy-to-use interfaces to build data security into enterprise applications
- Integrates data security seamlessly with application development and process automation infrastructure
- Allows decisions about data security mechanisms to remain in the hands of security experts, not in the hands of developers
- Enforces security consistently across applications through a defined security policy, not through code
- Allows security rules and mechanisms to change easily over time with minimal disruptions to deployed applications

RSA BSAFE® Data Security Manager tackles these problems by providing an architecture that balances the needs of security professionals to maintain control over security rules while meeting the corporate developers' requirement to implement strong data security in their applications. The major components of Data Security Manager are:

- The policy file – a "digital map" of sensitive data classifications mapped to the appropriate security mechanisms needed to protect them;
- Application interfaces – simple programming interfaces for developers to use inside applications to perform operations on sensitive data;
- Protection engine – the core of the product; it operates on data passed through the application. It interprets policy files and then applies security mechanisms to data based on its classification; and
- Security components – components that the protection engine calls on to implement security mechanisms such as encryption, digesting and digital signatures.

IMPLEMENTING GOOD SECURITY REQUIRES UNDERSTANDING YOUR DATA

RSA BSAFE Data Security Manager enables companies to get a good assessment of the sensitivity of their data sources and then assign classifications to that data. These classifications then become the basis for developing a policy file that maps them to the security mechanisms appropriate to secure that data. Classifications should only change when data types or needs change, not with every new application.

TRUSTED APPLICATION DEVELOPMENT MUST BE ACCESSIBLE TO ALL CORPORATE DEVELOPERS

Secure application development is becoming a key business requirement in many applications. Data Security Manager hides the complexity of security from developers, allowing them to stay focused on developing business logic. Implementing good data security is now accessible to any corporate developer, regardless of his or her skill set. Data Security Manager also integrates seamlessly with existing application development environments by supporting multiple languages and platforms—this enables corporate developers to get up to speed more quickly.



Confidence Inspired™

CONTINUED COMPLIANCE REQUIRES THE ABILITY TO ADAPT

How can companies adapt security policies over time as regulatory and business needs change without requiring changes to application code? RSA BSAFE® Data Security Manager addresses these issues by placing security decisions in the hands of security experts—those charged with developing and enforcing security policies. Security decisions are made and enforced by the security policy file. Developers do not have to know or understand these policies or the underlying security mechanisms because the rules defined will be enforced by the Data Security Manager. Also, each operation is logged so that security professionals can know that the rules they establish are followed consistently by every application.

KEY FEATURES

- Simple, high-level programming interfaces with bindings to multiple languages allow corporate developers to add security elements into new applications without an in-depth knowledge of cryptography or other security mechanisms.
- Makes appropriate security decisions based on policy and hides low-level security mechanisms from corporate developers. This helps them develop applications faster and build in the security elements in the design phase, right where they belong.
- Centralizes administration of data security policies, putting security decisions in the hands of security professionals—not developers—and enforcing consistent application of the policy by all applications using it.

- Auditable activity logs ensure consistent implementation of data security across applications, regardless of where it travels or resides. This aids regulatory compliance efforts.
- A broad range of security mechanisms provides flexibility to suit many environments and includes a number of different algorithms, ciphers and message digests to meet changing security and regulatory compliance needs.
- Support for legacy systems is provided through custom adapters for existing applications (offered through RSA Professional Services) to ensure that all legacy applications meet the same security policies and compliance requirements as new applications.
- Supports the FIPS 140 U.S. government standard, which specifies security requirements to be satisfied by a cryptographic module when used by a government agency.

DEVELOPMENT LANGUAGE SUPPORT

RSA BSAFE® Data Security Manager supports application development in C/C++, Microsoft C#, Microsoft Visual Basic, Microsoft Visual Basic.NET and Java.

PLATFORM SUPPORT

Supported platforms include Microsoft® Windows®, Red Hat® Linux®, Sun® Solaris™

Ports to mainframes and other platforms also available

ALGORITHM SUPPORT

Public key algorithms – RSA®

Symmetric ciphers (secret key), AES, RC5®, RC4®, RC2®, DES and 3DES

Message digests – MD2, MD5, SHA-1 and SHA-2

Message authentication codes – HMAC-MD5, HMAC-SHA1

Standards – x.509 v3, public key cryptography standards (PKCS) #7, FIPS 140 validated cryptographic module

