

Develop industry-standard secure, interoperable electronic mail applications.

TIPEM™ 2.0 RSA's S/MIME™ Toolkit



E-mail is the world's number one networked application. And it's rapidly becoming the primary way companies communicate with each other to conduct business online. Unfortunately, it's also one of the most vulnerable systems on the Internet. That's why more and more businesses require built-in security for their e-mail system.

But until now, e-mail security has been difficult to achieve. There have been a plethora of systems and "standards", most with very few available implementations, and almost none of which interoperate with each other. Buying a secure e-mail package meant being trapped into a single-vendor solution.

Until S/MIME.

Early in 1995, several major e-mail vendors got together with RSA to design a secure, interoperable messaging standard. They wanted to build on the predominant Internet messaging format, MIME (Multipurpose Internet Mail Extensions) and the PKCS #7 and #10 messaging standards. They wanted it to be easy to integrate, use and administer. They wanted to provide users with a mechanism to authenticate each other using globally-recognized X.509 digital certificates, or "digital IDs." And most of all, they wanted it to leverage the world's most trusted encryption technology: the RSA Public Key Cryptosystem™. What they built became known as the S/MIME standard.



S/MIME melds proven cryptographic constructs within the existing Internet MIME format to provide the best of both worlds — vigorous security in a system that guarantees readability of messages sent between different vendors' packages.

RSA's TIPEM 2.0 Toolkit

Using RSA's TIPEM 2.0, you don't need to be an encryption expert to provide state-of-the-art security features in your messaging package. With the TIPEM toolkit, developers can quickly and easily develop secure, interoperable messaging applications.

TIPEM 2.0 includes a comprehensive library of function calls to produce secure messages, including C object code modules for creating secure digital envelopes, digital signatures, and sophisticated X.509 certificate management functions.

The TIPEM 2.0 toolkit comes with an extensive library reference manual detailing all the cryptographic routines, as well as a complete, ready-to-run sample application with source code to assist in your development effort.

The toolkit is also re-entrant, a necessity in today's multitasking

operating environments. In addition, the toolkit optionally recodes binary data to ASCII and back, to provide for easy transport over any network.

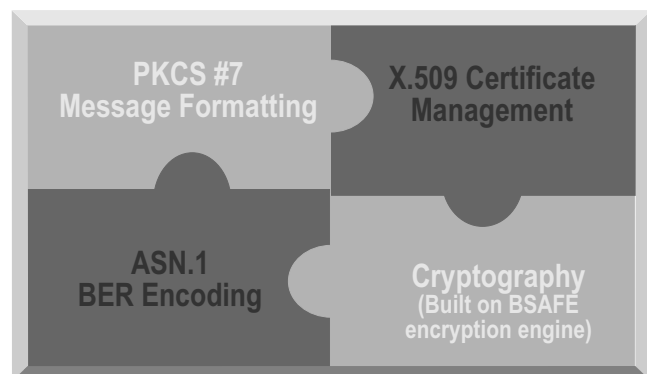
The Most Trusted Name in Security

Most importantly, TIPEM 2.0 is backed by the experience of the engineers and mathematicians of RSA Data Security, Inc., the recognized authority in public key encryption technology. When you come to RSA, you come to the source. The people who invented the world's most trusted encryption and authentication algorithms are the same people who will help you put this technology to work for you and your customers.

Written entirely in portable C, TIPEM 2.0 is available on a wide variety of platforms, and assembly language optimizations are included for many popular microprocessors. Source code and custom ports are always available.

How to get TIPEM 2.0

To purchase a copy of the TIPEM 2.0 toolkit, or if you would like more information on any of our products, please call an RSA representative at (415) 595-8782.



RSA's TIPEM 2.0 toolkit builds upon the proven BSAFE™ encryption engine to provide developers with a complete message processing platform.

TIPEM™ 2.0 Specifications

Features

- High-level cryptographic API designed specifically for S/MIME-compliant secure electronic messaging
- Certificate Management Extensions allow you to issue and track X.509 digital certificates
- Accepts standard X.509 v3 certificate extensions
- Supports ASN.1 BER encoding
- Portable C API, source licensing available
- Optionally recodes binary data into ASCII
- Interruptible and cancelable cryptographic operations
- Supports user-definable key sizes up to 2048 bits
- Supports the following cryptographic algorithms:
 - RSA Public Key Cryptosystem
 - Data Encryption Standard (DES)
 - Triple DES
 - RC2™ Variable Keysize Symmetric Block Cipher
 - RC5™ Variable Keysize Symmetric Block Cipher
 - MD5 Hashing Algorithm
 - SHA1 Hashing Algorithm
- Supports the Public-Key Cryptography Standards (PKCS)
- Hardware-specific assembly optimizations available

TIPEM 2.0 Applications

Developers can use the TIPEM engine for a whole range of secure messaging applications including:

- S/MIME-compliant secure electronic mail
- Secure Web-based messaging and forms
- Secure electronic forms routing and approval
- Secure workflow applications
- Can be used to create exportable secure messaging applications

System Requirements

Platforms:

- Windows 3.1, Win95, and Windows NT
- Unix
- Macintosh

(Many other platforms are available, please contact RSA for a current list.)

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 developing certificate formatting and parsing capabilities into their applications should examine BCERT, our toolkit specifically geared towards full-featured privacy and authentication applications requiring certificates.

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

TIPEM 2.0 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.



*With widespread industry support,
S/MIME™ is the standard for
secure internet messaging*

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.