

# S/PAY™

## RSA's Developer's Suite for Secure Electronic Transactions (SET)

The Internet, and in particular, the World Wide Web, offer enormous business opportunities for selling products and services online, anywhere, anytime, instantly. Up until now, however, the growth of digital commerce has been limited by the real and perceived shortcomings of security on the Internet.

### Enter SET

Jointly developed by MasterCard, Visa International and a consortium of other companies in conjunction with RSA, the widely-adopted Secure Electronic Transactions (SET) standard was specifically designed to address the security requirements of electronic transfers of credit and payment card information over open networks. With SET, Internet payment card transactions are actually safer than their traditional physical counterparts. Because SET relies upon strong cryptography based on RSA's widely accepted Public-Key Cryptography Standards and RSA digital certificates, consumers can be assured that their bankcard transactions will only occur in a secure, authenticated, and confidential environment.

### Developing SET-compliant applications

To enter this new market, you'll need a team of highly trained mathematicians and cryptographers, several experienced messaging protocol programmers and an administrative and development

team familiar with digital certificate processing, notarization policy and database management.

### Or, you could call RSA.

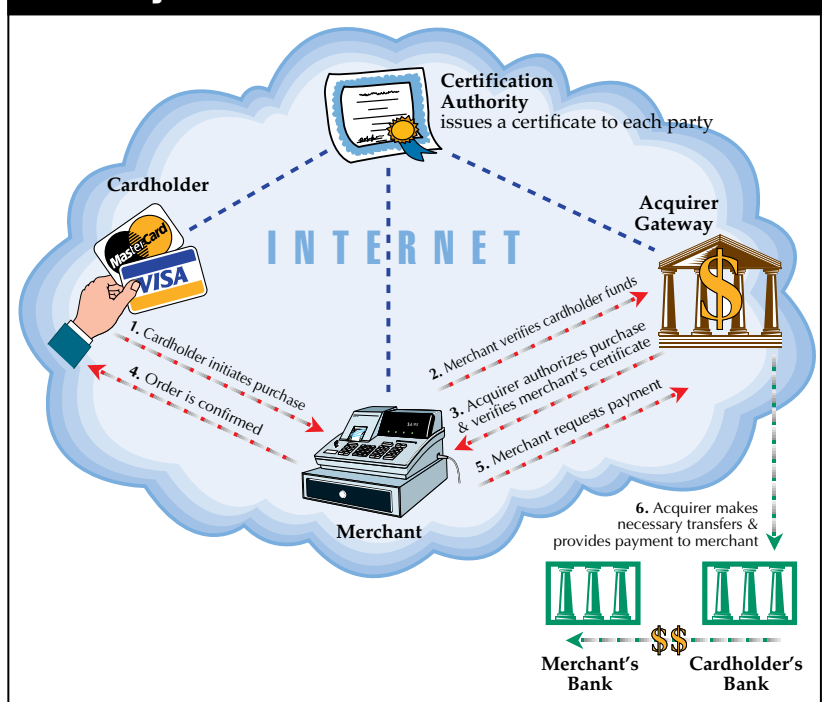
RSA's new S/PAY developer's suite makes developing SET-compliant applications easy. With a just little help from us, you can significantly streamline your development effort and get your SET product to market fast. And nobody knows security like RSA. We've built toolkits and security engines that are relied upon by the hottest development teams at companies like Microsoft, Netscape, Oracle, JavaSoft, and Intuit. With over 75 million copies of our crypto toolkits installed and in use worldwide, its little wonder we're called "the most trusted name in cryptography."

### Under the Hood

The S/PAY developer's kits provide a high level library for quick development of SET applications, sample code to illustrate the capabilities of each, and test tools to road-test and debug your SET cardholder, merchant, and acquirer applications. Multiprocessor and multi-thread safe, the S/PAY developer's kits provide developers with a comprehensive set of modules for SET-compliant cryptographic signing and enveloping operations. In addition, S/PAY's object libraries include certificate handling, SET transaction management and an interface to cryptographic devices. In short, everything you need to build and test virtually any SET-based application, server, or online service.



### The SET Payment Process



## RSA's S/PAY Developer's Kit Features

Each of RSA's S/PAY developer's kits for cardholder, merchant and acquirer applications provide the following functionality for development of powerful, coherent and interoperable SET products:

- **The SET Protocol Manager**

The SET developer's kits include a high-level library of all of the functions necessary to build SET messages. The C language API for each of these libraries can be called from both C and C++ environments.

- **PKCS Secure Message Processing**

S/PAY automatically encapsulates and formats messages according to the industry standard PKCS #7 secure messaging standard, which is specified by SET, providing the highest level of security and interoperability.

- **Shared Architecture**

RSA envisions that some developers may need to develop projects that entail a combination of cardholder, merchant, and/or acquirer applications. For this reason, each of the toolkits shares a common architectural framework, allowing developers to quickly move from one toolkit in the suite to another with little or no "learning curve."

- **Interoperability**

The RSA engineers who built the toolkits considered each and every critical component of the SET transaction, from cardholder initiation to final acquirer payment settlement transactions. All three developer's kits were extensively tested to guarantee developers cross-functionality and interoperability for any and all SET projects.

- **Cryptographic Operations**

The secret-key encryption, public-key encryption, message digesting, and digital signature algorithms included in the SET toolkits have been thoroughly researched, tested, and optimized by RSA's cryptographic engineers to provide you with the most secure and efficient implementations available.

- **Keypair Generation and Certificate Management**

SET certificates, modeled after the internationally recognized X.509 "digital ID's", play a crucial role in authenticating merchants, acquirers, and cardholders. Faulty or careless keypair generation can expose your company to liability – and properly requesting, verifying, and tracking the resulting certificates can be a difficult operation for the inexperienced. Each of the SET toolkits provides a sophisticated key generation and certificate request object module, as well as database support for managing certificates.

- **Thread Safety**

All the toolkits are multi-thread and multiprocessor safe, a key benefit in today's advanced, multiprocessor and multi-threaded environments. Mutual exclusion routines are used to protect data structures that are modified by two or more threads.

- **DER Encoding**

Messages in a SET transaction need to use the ASN.1 Distinguished Encoding Rules (DER), a complex and somewhat esoteric set of encoding specifications. S/PAY's developer's kits provide the necessary function calls and support to ensure that all messages follow the DER guidelines, automatically.

## RSA S/PAY: "Time to Market" Adv

In developing the SET developer's kits, RSA created a solution-oriented toolkit that contained a complete set of SET messaging protocols in SET. To ensure a timely protocol, RSA has partnered with the following companies to bring you the best of both worlds while still being the first to do so.

- **CRYPTOGRAPHIC HARDWARE SUPPORT**

**Atalla:** Atalla is working with RSA to develop an API for integrating hardware cryptographic support into SET-based applications as well as to integrate Atalla's PayMaster™ cryptographic processor with RSA S/PAY toolkits. The hardware API provides developers with greatly enhanced performance of cryptographic operations and physical protection of keys in merchant and acquirer products. The new RSA-based SET applications, with the strong security functionality and high throughput provided by Atalla's PayMaster Internet Security Processor (ISP), will help transform public networks such as the Internet into secure, high performance payment infrastructures.

- **CERTIFICATE SERVICES:**

**VeriSign:** Appointed by VISA to be the issuer of SET certificates on behalf of VISA member banks, VeriSign is working with RSA to ensure interoperability of VeriSign-issued SET certificates with the RSA S/PAY products. "RSA is taking a leadership position in making SET payments standards a reality by providing developers with cutting-edge encryption tools to build SET-capable applications," said Stratton Sclavos, president and CEO of VeriSign. "VeriSign intends to support this effort by providing these same developers with SET-compliant certificate services, incorporating RSA technology for bank, merchant, and cardholder solutions."

## Advantages and Global Distribution

Recognized the key importance of delivering a complete implementation of the security and, yet complete implementation of the SET software, hardware and financial service – a complete and powerful SET-engine,

- **WORLDWIDE FOCUS**

**NEC:** NEC is working closely with RSA and Nihon RSA, its Japanese subsidiary, to develop a Japanese SET standard enabling RSA to deploy its new developers' suite of solutions in Japan. In turn, this enables U.S. developers of RSA's products a higher degree of interoperability with their Japanese counterparts. NEC and Nihon RSA are also working on plans to develop specific cardholder and merchant solutions for the Japanese marketplace using RSA's S/PAY developer's kits.

- **EXPORTABILITY**

For the first time, a toolkit that incorporates strong encryption and signing keys – RSA's S/PAY developer's kit – has been approved for export by the U.S. Departments of State and Commerce. By focusing specifically on the SET protocol, and by limiting the strong cryptographic functions to SET-specific financial messages, the use of long cryptographic key lengths was not considered a security risk by the applicable U.S. government agencies. Now, application developers worldwide can get access to RSA's domestic cryptographic toolkit that implements full 56-bit DES secret keys, and 1024-bit RSA key exchange keys for use in their SET-based applications.

## Time-Saving, Flexible Architecture

SET development projects can appear deceptively simple. Under closer examination, however, building a SET engine that generates, requests, manages and tracks hundreds of distinct messages and routines, thousands of times a second, can quickly become overwhelming.

The RSA S/PAY developer's kits were specifically designed to handle the SET message and data structures so you don't have to. RSA's engineers have built in the cryptography, certificate infrastructure, transaction integrity and SET messaging framework so you can concentrate on developing your application – not the security behind it.

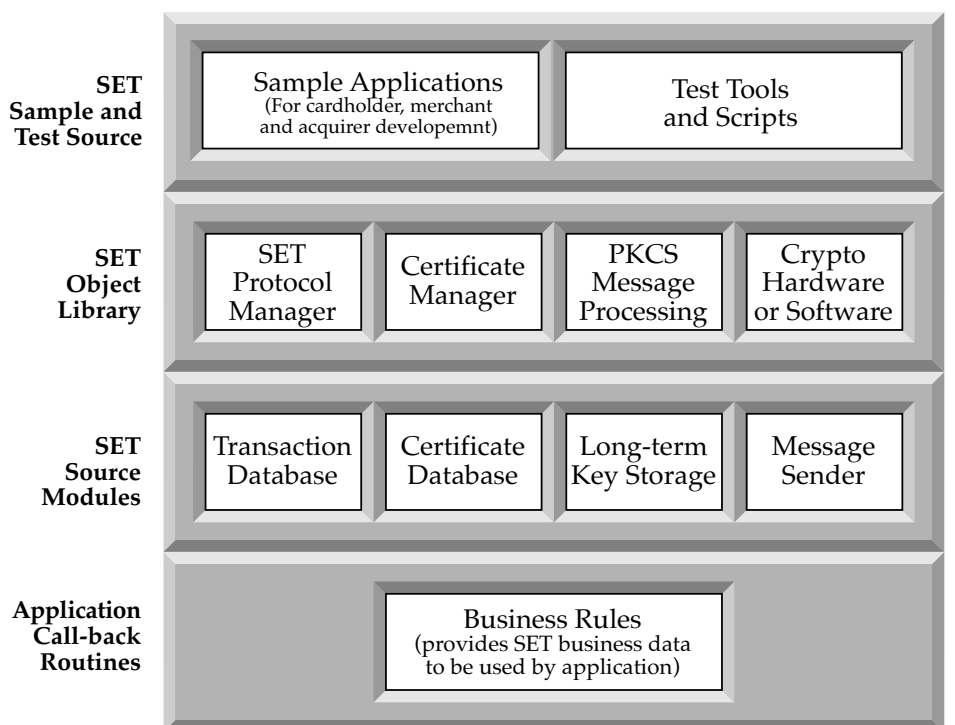
The components of each of the S/PAY kits is optimized for its target environment – each toolkit has unique and specific source code modules for SET sample code, testing scripts, database support, long-term key storage, and message processing (see diagram below). At the same time, each developer's kit shares a common core of cryptographic and SET

message object libraries, allowing your developers to switch from kit to kit without having to learn a whole new interface.

This approach streamlines cross-development and ensures interoperability across client, merchant and acquiring institution applications. Furthermore, by "burying" all cryptographic routines deep within the toolkits, and providing others only as SET-specific object code, RSA can offer a single, consistent tool suite for use worldwide – with full cryptographic strength. That means with S/PAY, you'll be able to develop and deploy secure, interoperable payment applications in markets around the world.

Designed from the ground up to be simple, easy-to-use, and efficient, S/PAY's high level API provides a robust and full implementation of the entire SET specification for each and every SET message. Adaptable to multiple environments, the toolkits are also multi-thread and multiprocessor safe, a necessity in today's advanced multitasking and multiprocessor environments.

### RSA S/PAY Developer's Kit Architecture



---

# S/PAY™ 1.0 Specifications

## Features

- Optimized performance for cardholder, merchant, and acquirer applications
- High-level API gives developers an intuitive interface to the complex security algorithms underlying SET
- Easily interfaces to a variety of cryptographic hardware devices
- SET Certificate Management object code allows you to easily request, exchange, verify and track SET digital certificates
- Core cryptographic functionality facilitates development of exportable SET applications
- Secure, long-term private key storage facilities
- Multiprocessor and multi-thread safe
- Interruptible and cancelable cryptographic operations
- Supports the following cryptographic algorithms:
  - RSA PKCS #1 Signatures
  - RSA w/OAEP
  - DES
  - CDMF DES
  - SHA-1 Hashing Algorithm
- Business rules, database interface and application call-back routines provided in source code for easy customization
- Supports ASN.1 DER encoding

## S/PAY Applications

Developers can use the SET cardholder, merchant, and acquirer engines for a whole range of secure electronic commerce projects including:

- Web-based secure “stores” and electronic malls
- Secure merchant servers
- Secure payment gateways
- Plug-ins and additions to Internet browser and server applications
- Online banking services and applications
- CD-ROM based catalogues
- Exportable secure electronic transaction 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, RSA's general purpose modular cryptographer's toolkit.

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

Users developing certificate formatting and parsing capabilities into their applications will need BCERT, our toolkit specifically geared towards certificate management applications.

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

## S/PAY Pricing

RSA offers several S/PAY pricing plans to accommodate high volume OEMs, low volume redistribution, and non-commercial development uses. Every customer should find a flexible pricing plan to suit their business and development needs. For specific pricing information, developers are encouraged to call RSA Sales at (415) 595-8782. OEM discounts and site licensing pricing are also available.

---

## Contacting RSA



RSA Data Security, Inc.  
100 Marine Pkwy Ste. 500  
Redwood City, CA 94065  
Phone: 415-595-8782  
Facsimile: 415-595-1873  
<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.