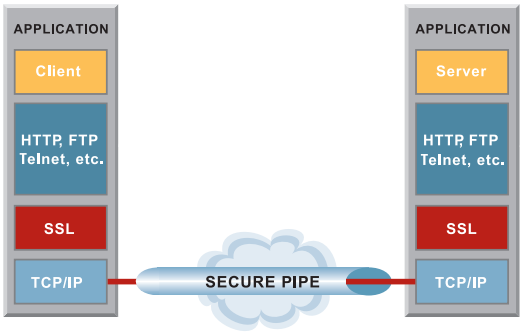
Security Protocols Overview *An RSA Data Security Brief*

SSL & TLS

Secure Socket Layer & Transport Layer Security

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 are able to authenticate each other and to establish a secure link, or "pipe," across the Internet or Intranets to protect the information transmitted.



The Need for SSL

With the growth of the Internet and digital data transmission, many applications need to securely transmit data to remote applications and computers. SSL was designed to solve this problem in an open standard.

SSL is analogous to a secure "telephone call" between two computers on any network including the Internet. In SSL, a connection is made, parties authenticated, and data securely exchanged. The latest enhancement of SSL is called Transport Layer Security (TLS).

Algorithms

In applications using SSL, the confidentiality of information is ensured using strong encryption technologies. Through the use of digital certificates, SSL provides the transparent authentication of servers and, optionally, clients as well. SSL uses the RSA algorithm as the algorithm to enable security using digital signatures and digital enveloping. For very fast encryption and decryption of data for transmission after an SSL connection has been established, the RC4® algorithm is the preferred algorithm. Other algorithms are available in the SSL specification as well.

Based on the strong cryptography in SSL, users have confidence that their information is confidential, authentic, and original during a network connection.

Why Isn't SSL in the Browser Enough?

While SSL is used on the Web for many applications, situations often demand that SSL in the browser is not enough. For example, if one end of the connection is not SSL-enabled or Web-enabled, then tools are needed to build SSL into the application. Other situations require that applications have more control over connections including the selection of cipher suites and key negotiation. Developers who use the SSL contained in the Web browser have little control over SSL performance and operation.

SSL versus IPSec

IPSec secures the low-level network packets in order to create a secure network of computers over insecure channels, including the Internet and leased lines. SSL operates at the transport layer, abstracted from the network layer where IPSec operates. SSL operates between any two applications that do not necessarily need to be on the same secure network. Where SSL secures two applications, IPSec secures an entire network.

Applications

SSL can be used in any situation where a link between two computers or applications needs to be protected. The following are just a few of the real-world, practical applications of SSL & TLS:

- **Client/Server Systems**

  SSL in the browser is not enough to secure most systems. Systems such as secure database access, or remote object systems such as CORBA, can all be securely improved using SSL. Other applications include redirection of secure connections such as proxy servers, secure Webserver plug-ins, and Java "Servlets."

- **Financial**

  Banks and financial companies can use SSL to develop remote banking programs that employ strong cryptography. Some applications that operate outside of the Web browser allow customers to check account balances, transfer funds, or even apply for a new mortgage without speaking to a loan officer.

- **Information Systems**

  Many systems employ SSL to create remote access and administration applications. Using SSL, it is easy to create secure remote access and control systems for management of system activity and resources.

- **Travel Industry**

  SSL can be used to create online reservation systems and secure information transfer. Organizations who build SSL-enabled applications can allow their customers to securely book reservations online without ever speaking to a sales person.

RSA Data Security Products that Support SSL & TLS

RSA BSAFE™ SSLJ SECURITY PROTOCOL COMPONENTS FOR JAVA

RSA BSAFE™ SSLC SECURITY PROTOCOL COMPONENTS FOR C

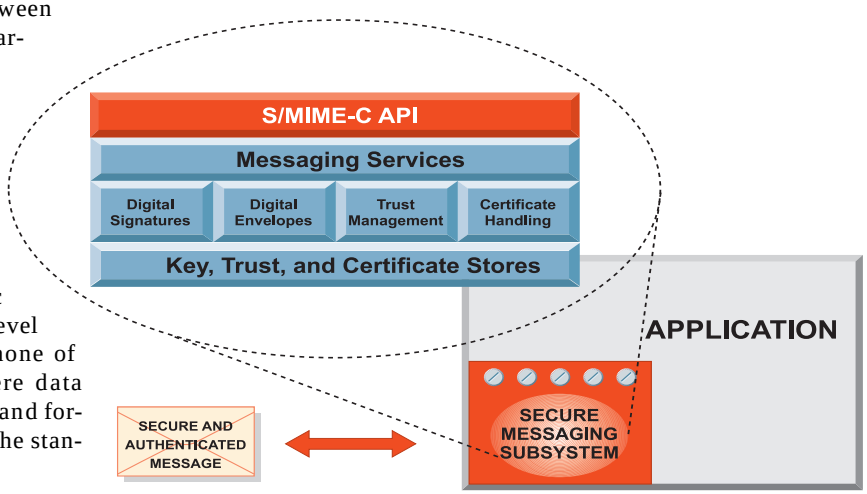
Security Protocols Overview *An RSA Data Security Brief*

S/MIME

Secure Multipurpose Internet Mail Extensions

S/MIME is the electronic messaging standard that enables e-business by addressing the important issues of data privacy and authenticity. S/MIME uses public-key encryption technology to protect messages from unauthorized interception and forgery.

An S/MIME-enabled application is analogous to a secure piece of postal mail travelling between two locations. The S/MIME protocol guarantees the secure transmission, storage, authentication, and forwarding of secret data.



The Need for S/MIME

Protocols such as SSL and TLS provide security at the application level for communication between hosts on a public network. Other protocols, such as IPSec and others, maintain the security of low-level network communications. However, none of these protocols handle situations where data needs to be securely stored, transmitted, and forwarded. In this area of use, S/MIME is the standard.

S/MIME versus SSL

Where SSL secures a connection between a client and a server over an insecure network, S/MIME is used to secure messages between users, applications, and computers.

Algorithms

S/MIME based on the RSA algorithm for digital signatures and digital envelopes. The RC2®, DES, and Triple DES algorithms are utilized for symmetric encryption. For hashing, S/MIME is based on the MD5™ and SHA1 hash algorithms.

Applications

S/MIME is applicable to any situation in which data must be securely transferred, stored, forwarded, and authenticated. The following are just a few of the real-world, practical applications of S/MIME:

- **Electronic Data Interchange**

  S/MIME is used as a basis for EDI-INT, the Internet standard for EDI over the Internet. These applications include digital signatures on contracts and secure data interchange over the Internet.

- **Financial Messaging**

  Organizations can use S/MIME to store and transfer bank statements and financial forms between computers. Other uses include transfer of stock trades, communication of brokerage statements, and mortgage payment services.

- **Content Delivery**

  S/MIME can be used to implement electronic bill presentment and payment online. Customers using applications based on S/MIME can securely receive and pay their bills without any stamps. Other applications include online software sales and subscription services.

- **Healthcare**

  Healthcare providers can use S/MIME to create secure patient records and health claims. Providers can build S/MIME enabled applications that remove the overhead of patient record management inherent in antiquated record storage techniques.

RSA Data Security Products that Support S/MIME

RSA BSAFE™
S/MIME C
SECURITY PROTOCOL COMPONENTS FOR C

IPSec

IP Security Protocol

IPSec is the leading standard for cryptographically based authentication, integrity, and confidentiality services at the IP datagram layer. IPSec comprises a basis for interoperably secured host-to-host pipes, encapsulated tunnels, and Virtual Private Networks (VPNs), thus providing protection for client protocols residing above the IP layer.

IPSec ensures that the low-level IP packets that are continuously transferred between computers on a secure network are unaltered, authentic, and private.

The Need for IPSec

At the IP layer, computers on a network communicate by routing datagram "packets." These datagrams contain data, destination addresses, source addresses, and other information. In a conventional network configuration such as corporate local area networks (LANs), these datagrams are passed "in the clear." There is nothing to stop a malicious attacker from hijacking, forging, and modifying these packets.

Generally, physical security and Internet firewalls prevent attackers from outside of the LAN from mounting an attack on conventional networks. However, in situations such as the Internet and any other unsecured network, there is little to stop an attacker from intercepting, forging, or modifying datagram packets.

Algorithms

IPSec is based on the Diffie-Hellman and/or the RSA algorithms for key exchange. For symmetric encryption, the DES and Triple-DES algorithms are utilized. In situations where greater security is required for encryption in IPSec, the RC5™ algorithm is commonly used. For hashing, the SHA1 hash algorithm and MD5™ are used.

IPSec versus SSL

IPSec secures the low-level network packets in order to create a secure network of computers over insecure channels, including the Internet and leased lines. SSL operates at the transport layer where they do not need to be located on the same secure network, but are instead used to ensure security between applications across an public network. Where SSL secures two networked applications, IPSec secures an entire network.

Applications

IPSec is applicable to any situation in which secure network communication is desired over insecure networks such as the Internet. The following are just a few of the practical, real-word applications of IPSec:

- **Virtual Private Network (VPN) Software and Hardware**

  Many organizations use the IPSec standard to build software that enables Virtual Private Networks. This can be used to create secure networks over insecure means of transmission such as the Internet. Using VPNs, companies can save money in terms of the costs of leased lines while maintaining the confidentiality of corporate information.

- **Remote Access Software and Hardware**

  Remote access software based upon the IPSec standard provides enterprises with secure access to their network functions. Remote access hardware provides another level of security not found in software enabling remote access to the network resources.

- **Firewall Products**

  Firewall products can easily incorporate IPSec to create secure VPN network tunneling. These products allow corporations to easily create secure and cost-effective links with their business partners and members of the enterprise.

RSA Data Security Products that Support IPSec

RSA BSAFE™ Crypto-C and RSA BSAFE™ Crypto-J are products that provide the core cryptography needed to implement IPSec and VPN systems.

Corporations such as Cisco, Bay Networks, IBM, Raptor, and Secure Computing have all incorporated IPSec and the RSA BSAFE™ Crypto-C or RSA BSAFE™ Crypto-J security components into their products.

RSA BSAFE™ Crypto C
CRYPTOGRAPHIC COMPONENTS FOR C

RSA BSAFE™ Crypto J
CRYPTOGRAPHIC COMPONENTS FOR JAVA

Security Protocols Overview *An RSA Data Security Brief*

Security Protocols

A number of different security protocols have been introduced. The following table summarizes the most popular security protocols and the RSA product that developers should use to implement them:

Protocol	Summary	Algorithms	RSA Product
CDPD (Cellular Digital Packet Data)	Standard designed to enable customers to send computer data over existing cellular networks.	DH, RC4®	BSAFE™ Crypto-C, BSAFE™ Crypto-J
DNSSEC (Domain Name System Security Extensions)	Protocol for secure distributed name services such as hostname and IP address lookup.	RSA, MD5™, DSA	BSAFE™ Crypto-C
DOCSIS (Data Over Cable Service Interface Specification)	Cable modem standard for secure transmission of data with protection from theft-of-service and denial-of-service attacks and for protecting the privacy of cable customers.	RSA, DES, HMAC, SHA1	RSA BSAFE™ Crypto-C
IEEE 802.11	Protocol standard for secure wireless Local Area Network products.	RC4®, MD5™	RSA BSAFE™ Crypto-C, RSA BSAFE™ Crypto-J
IPSec (IP Security Protocol)	Standard for cryptographically-based authentication, integrity, and confidentiality services at the IP datagram layer.	RSA, DH, MD5™, DES, 3DES, SHA1	RSA BSAFE™ Crypto-C, RSA BSAFE™ Crypto-J
PPTP (Point-to-Point Tunneling Protocol)	Used to create Virtual Private Network communication across the Internet; works at the IP Datagram layer.	RSA, DES	RSA BSAFE™ Crypto-C
SET (Secure Electronic Transactions)	Allows secure credit card transactions over the Internet.	RSA, SHA1, DES, HMAC-SHA1	Trintech's S/PAY, RSA BSAFE™ Crypto-C
S/MIME (Secure MIME)	Guarantees the secure transmission, storage, authentication, and forwarding of secret data at the application level.	RSA, DES, 3DES, RC2®, MD5™, SHA1	RSA BSAFE™ S/MIME-C
SSH (Secure Shell)	Protocol that permits users secure remote access over a network from one computer to another.	RSA, RC5™, RC4®, RC2®, DES, 3DES	RSA BSAFE™ Crypto-C, RSA BSAFE™ Crypto-J
SSL & TLS (Secure Sockets Layer & Transport Layer Security)	Allows a "secure pipe" between any two applications for secure transfer of data and mutual authentication	RSA, RC4®, SHA1, MD5™, 3DES, DES, DH	RSA BSAFE™ SSL-C, RSA BSAFE™ SSL-J

Copyright © 1999 RSA Data Security, Inc. All rights reserved. RSA BSAFE , RC2, RC4, RC5, and MD5 are trademarks or registered trademarks of RSA Data Security, Inc. All other trademarks are the property of their respective owners.