Introduction
Using Security in Mosaic
Security menu options

SPRY Mosaic implements the S-HTTP standard of privacy and encryption to allow secure transactions over the Internet. SPRY Mosaic uses **SecureWeb**™ Secure HTTP transaction security technology from Terisa Systems.

Using S-HTTP, SPRY Mosaic allows you to:

- send and receive encrypted messages
- digitally sign messages you send to a remote server
- view digital signatures on a remote server to authenticate the identity of the remote server

Secure transactions in Mosaic, such as sending and receiving encrypted data or viewing or submitting digital signatures, will occur when you are connected to an S-HTTP server. An S-HTTP server can be identified by a URL that begins with **shttp://**. These servers **cannot** be accessed directly, but must be reached indirectly through links from other documents.

Currently, there are few S-HTTP servers in existence. **Internet Office Web Server** is an S-HTTP Web server for Sun, HP, UNIX and Windows NT platforms. For more information on Internet Office Web Server, see the following Web page: **http://www.spry.com/sp_prod/officeserver/index.html**.

 Where to Learn More

For Information on:	See this Web page:
Cryptography Concepts	**ftp://rsa.com/pub/faq.asc**. A frequently asked questions (FAQ) document on cryptography, and provides a fairly thorough background on secure transaction technology.
Secure HTTP	**http://www.eit.com/projects/s-http/index.html** A good collection of technical and non-technical documents about S-HTTP.
RSA's Commercial Certificate Authority	**http://www.rsa.com** Information on RSA's Commercial Certificate Authority.

 **Introduction**

 **Using Security in Mosaic**

Overview

Logging into a key database

Viewing encrypted information

Sending encrypted information to a server

Viewing digital signatures

Creating a key

Signing with a key

Using a shared key

 **Security menu options**

SPRY Mosaic supports several methods of S-HTTP security: **shared key encryption**, **public key encryption**, and **authentication** using digital signatures. Click below for examples of different types of secure transactions in Mosaic.

- Shared Key Encryption
- Public Key Encryption
- Authentication

Rufus College wants to allow students to access schedule information on the World Wide Web. The college wants to ensure that only a registered student can view his or her schedule, so they might set up shared keys, a method of encryption similar to a traditional password scheme. Both ends of a transaction (college and student) know a **shared secret** or password. The student must provide the shared key (which contains the shared secret) to the college server before the schedule is shown.

NOTE Shared keys are not always a secure method of cryptography, since the secret can be used by anyone who knows it, and there is no verification of the identity of the sender.

Morbid Flowers, Inc., wants to allow customers to provide their credit card numbers so that they can order flowers over the World Wide Web. They want to assure their customers that the credit card information cannot be read by anyone else. Morbid Flowers generates a **public** and **private** key pair; the public key is known, but the private key is stored only on Morbid Flowers system, in an encrypted format.

When a customer wants to send credit card information to Morbid Flowers, he or she clicks a Submit button on the order form, which encrypts the information with Morbid Flowers' public key. Since the associated private key is required to read the message, only Morbid Flowers can decrypt the message. If the message (credit card information) is intercepted by someone else, it cannot be decrypted, provided Morbid Flowers has kept their private key secure.

The Heraldry Club wants to make sure that only members in current standing can access its heraldry database. The Heraldry Club can require that requests for information carry digital signatures which vouch for the identity of their members. Members are prompted to "sign" database access requests before they are sent.

You can also view the digital signature of a Web page, in order to be sure that page is legitimate. For instance, customers buying flowers from Morbid Flowers, Inc., may want to make sure that Morbid Flowers is a legitimate company, and that they are actually sending their credit card information to Morbid Flowers, and not to another company or individual.

Show Me

Mosaic stores public and shared key information in key databases stored on your local PC. Any time you want to add new security information to Mosaic, or use security features in Mosaic, you will be required to log into a key database.

To log into a key database:

1. Click Key Database Login on the Security menu; you will see the Key Database Login dialog box.
2. In the **Username** box, type the name for the key database. If you specify a new name, a new key database will be created.
3. In the **Password** box, type the password for the database. If you are creating a new key database, be sure to record your password information; this information cannot be retrieved.

You can create as many databases as you wish, although you may find it useful to use just one database. Once you log into a key database, all new security information that you define when you are logged in will be stored in that database; you will not be able to log into another key database until you exit and restart Mosaic.

You can change the password for the current key database at any time; click **Change Password** on the **Security** menu. You will have to provide your old password before you will be able to supply a new password.

Note that as long as you are logged into your database, anyone can use the security features in SPRY Mosaic and can perform transactions "in your name". If you want to ensure that this does not happen, close Mosaic when you leave your PC; no one will be able to use security features without first logging into the database.

Some S-HTTP servers will allow you to encrypt information so that it can be decrypted and viewed only by the server to which it was sent. Most, but not all, secure servers will give you some indication when information you provide them will be encrypted. You can tell that the information is being encrypted if the Mosaic logo (to the right of the toolbar) changes to a combination lock logo after you submit information:

Note that you may want to check the digital signature of a document before sending sensitive information to that server.

SPRY Mosaic can display encrypted S-HTTP Web pages. An envelope icon on the right hand side of the Mosaic status bar will indicate that the Web page you're viewing is encrypted.

Some Web pages may be "signed" with a digital signature. **CERT** displayed on the right hand side of the Mosaic status bar will indicate that a document has been digitally signed and certified.

Positioning the cursor over **CERT** will display the Distinguished Name of the signer, or “owner,” of the displayed Web page, in the status bar. Clicking on the envelope icon will display a Public Key Certificate dialog box displaying full information about the certified key of the signer.

Some servers may require you to provide a key as proof of your identity before you will be allowed to perform a transaction or before you will be allowed to view information. Creating a usable key involves several steps, described below.

To obtain a key that you can use to sign documents:

1. Select New Key Request from the Security menu.
2. Fill out the New Key Request dialog box with the information required by the Certificate Authority. If you are requesting a Persona Certificate, you will only need to fill out the **Common Name** box.
3. Specify a filename and location for the key request file. The default name (keyreqst.txt) is suggested.

   A key will be generated for you. The first time you generate a key, you may be asked to move your mouse around the screen in order to provide "random information" for Mosaic's random number generator. You will receive a message indicating that the key was generated, and the file you specified will be created.
4. You now have to submit your certificate request to a Certificate Authority. The method used to submit your request will vary depending on the Certificate Authority you are using. If you are requesting a Persona Certificate, see the instructions below.

   Requesting a Persona Certificate:

   You can request and receive a Persona Certificate via e-mail. Mail the key request file you created to **persona-request@rsa.com** in the body of your mail message (not as an attachment). You can use any text you want in the message subject. (If you are using **SPRY Mail** to mail the request, click Insert Text File on the Edit menu, and specify the name and location of the key request file.)

   RSA will mail you a certificate by e-mail reply. This is usually a quick turnaround; you may get a reply in as little as five minutes. When you get the reply, you should save the message to a text file. (In SPRY Mail, choose **Save** from the **File** menu.)
5. When you have received a certificate from a Certificate Authority, click Add Certificate on the Security menu and specify the location of the certificate file.

   The secure key is now created, and should display in the Public Keys dialog box. You can now sign documents with the key you created.

You can sign documents with a key in order to verify your identity. When you reach a server that requires a signature, the Public Keys dialog box appears, displaying any keys you created. Choose the key you want to sign with from this dialog box, and click **OK**. The key will be used to sign the document.

See Also

Creating a key

Some servers require you to supply a shared key in order to access information. If you have already set up key information, a Shared Keys dialog box will appear, prompting you to select a shared key to use.

If the key you want to use is shown, highlight the key you want to use and click **OK**. (If you have not yet created the shared key, and need to create one, click the **New** button, the New Shared Key dialog box will appear.) If the key you select is correct, the information you requested will appear.

If you have never set up any shared keys, the New Shared Key dialog box will appear, prompting you to create a new shared key.

Introduction
Using Security in Mosaic
Security menu options
Key Database Login
Change Password
New Key Request
Add Certificate
Public Keys
Shared Keys
Trusted Roots

Logs into a key database, so that you can add new security information to Mosaic, or use security features in Mosaic. You can also create a new key database using this dialog box.

Username	Specifies the name for the key database. If you specify a new name, the key database will be created.
Password	Specifies the password for the database. If you are creating a new key database, be sure to record your password information; this information cannot be retrieved.

Changes the password for the current key database. You will have to provide your old password in order to change your password.

Old Password	Specifies your current password.
New Password	Specifies the password you want.
Retype Password	Confirms the password you typed in the New Password box.

Generates a request for a certified key to use for secure transactions in Mosaic. This request is saved to a file that you can submit to a Certificate Authority.

If you are requesting a Persona Certificate from RSA, you should only fill out the **Common Name** box. If you are using a different Certificate Authority, you may need to fill out additional information, depending on the Certificate Authority and the type of Certificate you are requesting.

Key Length	Specifies the length of keys that are generated. The default key length is 512K. Longer keys take more time to generate but are harder to "crack". Note that keys larger than 512K will not interoperate with servers outside of the U.S. and Canada.
Validity Period	Specifies how long the key will be valid before expiring. Different Certificate Authorities will allow you to specify different validity periods. After the validity period is over, you will not be able to use the key associated with this certificate.
Common Name	Specifies a unique name. This should be **your** name, not the name of your business, school or other institution, since this has to identify you uniquely and will be part of your digital signature. You can use your full name, if you wish; your e-mail address is also recommended, since it is always unique. Bear in mind that once you create a key with this name, you will not be able to create another key with this name until the end of the Validity Period, so if you are planning to create several keys, choose the common name carefully. **This is the only field you need to fill out if you are requesting a Persona Certificate from RSA.**
Organizational Unit	This is the name of the unit within the organization that will be generating your certificate. The value for this field will vary depending on the type of certificate and Certificate Authority that you request; if you are requesting a Persona Certificate, **you should not change this field**.
Organization	This is the organization which will be generating your certificate. The value for this field will vary depending on the type of certificate you request and the Certificate Authority you use; if you are requesting a Persona Certificate, **you should not change this field**.
Locality	This is your city. If you are requesting a Persona Certificate from RSA, **you should not fill out this field.**
State or Province	This is your state or province. If you are requesting a Persona Certificate from RSA, **you should not fill out this field.**
Country	This is your country. If you are requesting a Persona Certificate from RSA, **you should not change this field.**

See Also

Creating a key

Adds a certified key to the current key database. You must have a certificate file from a Certificate Authority, in text file format.

Displays any certified keys you have added to Mosaic (see Creating a key for information). This dialog box appears whenever you reach a server that requires you to sign a document with a key, or when you click Public Keys in the Security menu.

You can get information about a key by double-clicking the key name, and can sign a document with a key by selecting the key and clicking **OK**.

You can also delete keys from Mosaic by selecting the key and clicking the **Delete** button. Be careful when deleting keys as they will be permanently removed from your system and you will not be able to recover them.

Displays any shared keys you have added to Mosaic. Shared keys are required to access certain secure servers. This dialog box appears when you reach a server that requires you to access information using a shared key, or when you click Shared Keys in the Security menu.

If you are prompted to supply a shared key, choose the shared key from this dialog box, and click **OK**.

New	Launches the New Shared Key dialog box, allowing you to add a new shared key.
Delete	Deletes the selected shared key. Be careful when deleting keys as they will be permanently removed from your system and you will not be able to recover them.

Creates a shared key that can be used to access a secure server.

Username	Specifies a name for the shared key. This value should be provided by the secure server administrator (it is used when verifying your key).
Secret	Specifies the secret portion of your shared key. This value should be provided by the secure server administrator (it is used when verifying your key). This text is hidden as you type and does not display in any dialog boxes.
Host	Specifies the IP address of the server where this shared key will be used. (This value is optional.) If you specify this value, you will not see this key unless you are asked for a key on that host.
Port	Specifies the port on the Host (above) where this key will be used. As with Host, you will not see this key unless you are asked for a key on that port of the host.
Description	Specifies a description for this key. (This value is optional).
Save this Key Permanently	Sometimes you may just need to use a key one time. If you plan to access the encrypted information again, you should check this box so that the shared secret will be stored in your key database.

Displays Certificate Authorities that you have defined as trusted roots. Documents must be signed with certificates from these trusted roots before you will accept their signatures as valid.

Three trusted roots from RSA Data Security, Inc. are pre-defined in SPRY Mosaic: the Secure Server Certification Authority, the Commercial Certification Authority and the Low Assurance Certification Authority.

Add Adds additional trusted roots. You will have to specify the filename of a certificate file from the Certificate Authority.

NOTE If you are getting "Cannot Create Certificate Chain" messages when trying to access a secure Web page, it may be because you do not have the Certificate Authority that was used to sign that page defined as a trusted root.

Displays certificate information for the holder of a certificate.

Distinguished Name	Identifies the Common Name (CN) (unique identifier for the person or organization holding the certificate), Organizational Unit (OU) (the type of authentication), Organization (the organization vouching for the identity of this person or organization) and Country for the certificate.
Status	Indicates whether the certificate checking includes Certificate Revocation List (CRL) checking. This is not currently supported in SPRY Mosaic.
Validity Period	Specifies the date that the certificate will expire. Certificates are only valid for a certain length of time. When the certificate has expired, it will no longer be usable for secure transactions.
Certification Chain	Displays the Organizational Unit, Organization, and Country for any Certificate Authorities that issued this certificate.

Glossary items

Certificate Authority

An organization that verifies the identity of users on the World Wide Web. Before you can use a key for secure transactions in Mosaic, you must have the key certified by a Certificate Authority.

Some Certificate Authorities require you to identify yourself before issuing a certificate; they may require you to appear in person and show identification such as a birth certificate or passport, or sending identification via U.S. Mail. These organizations usually require a fee. There are also low assurance Certificate Authorities that issue certificates without a high level of verification.

SPRY Mosaic is set up to allow you to request a **Persona Certificate** from **RSA Data Security, Inc**. A Persona Certificate can be requested and issued over e-mail, and therefore offers only a low assurance level of certification. Many transactions will require a higher level of certification than a Persona Certificate.

certificate

Since anyone can generate a public/private key pair, there must be some way to authenticate a person's identity. Certificates are documents that include a user's public key and have been signed by Certificate Authorities, organizations that attest to the identity of the person with that public key.

A certificate is like a form that has been signed by a notary public; in this case, the Certificate Authority is the "notary public" for the certificate and attests to a person's identity. Certificates become part of digital signatures, so that identities can be verified by checking the certificate information associated with a signature.

digital signature

A method used to authenticate messages; a digital signature accompanies the message, and serves as verification that the message was sent from a specific source. Digital signatures include **certificate chains**, which show which Certificate Authorities have vouched for the identity of the signed document.

Digital signatures can also authenticate a message's integrity; once a message is signed, if any part of the message is altered, the message will not be recognized as valid.

key database

A database that stores all your public and shared key information. You can have as many key databases as you wish; you have to log into a key database before you will be able to use the keys in that database.

A key database is saved in your \DATA directory (under the Mosaic installation directory) in three files: **username.key**, **username.pag**, and **username.dir**, where **username** is the name you specified for the key database. The information in these files is encrypted, and

can only be viewed by supplying a password in Mosaic.

Persona Certificate

A low level of certification, provided by RSA Data Security, Inc. These certificates are not generally recommended for secure transactions, as there is no formal proof of identity required to obtain a Persona Certificate.

public key encryption

A method used for encrypting and decrypting messages which uses public and private key pairs in order to ensure security.

A pair of numbers is generated using a sophisticated generation scheme involving prime numbers. One of these numbers, the **private key**, is kept secret, and is never transmitted over the Internet. The other number, the **public key**, is available to others.

Although the private key cannot be derived from the public key (and vice versa), there is a scheme by which the two numbers can be matched. This means that a message encrypted using the **public** key can only be decrypted by the holder of the private key**.** This ensures that a message can be encrypted so that only one user can read it.

Likewise, public and private keys can be used to create and verify digital signatures that uniquely identify messages as having come from a specific person. Digital signatures can be used to provide reliable authentication that can not be disputed.

shared key

Shared keys are a method used for low-level encryption and authentication. A server will require a person to provide a **shared secret** in order to access server information. A shared secret is much like a password; it is a piece of information known by both sides of a transaction.

You will not be able to access the protected information unless you know the shared secret for that information. This will be provided to you by the site you are trying to access, if they want you to access their information.

trusted root

You can specify that Mosaic display only secure pages signed by one or more particular Certificate Authorities. These Certificate Authorities are known as trusted roots. Web pages must be signed with the certificate from a trusted root before you will accept their signatures as valid.

Three trusted roots from RSA, Inc., are pre-defined in Mosaic: the Secure Server Certification Authority, the Commercial Certification Authority and the Low Assurance Certification Authority. You can display and add trusted roots by choosing **Trusted Roots** from the

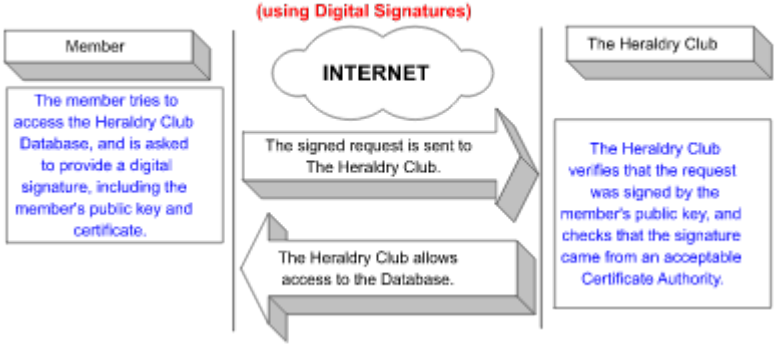
Security menu.

You can add additional trusted roots if you have a certificate file from the Certificate Authority.

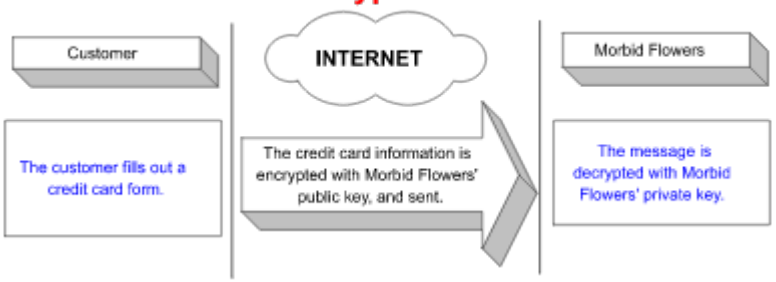
NOTE If you are getting "Cannot Create Certificate Chain" messages when trying to access a home page, it may be because you do not have the Certificate Authority that was used to sign that home page defined as a trusted root.

Diagrams

Authentication
(using Digital Signatures)



Encryption



Shared Keys