



Security Tutorial

Version 2.4

© 1999/2000, Bolero International Ltd., all rights reserved.
This publication contains proprietary and confidential information. The recipient cannot disclose this information to third parties without the written permission of Bolero, nor use it for purposes other than those agreed upon with Bolero.

Certification Tutorial

Why do I need digital security?

In your business today, you send and receive trade information by post, fax and, increasingly, by email. But are you certain that the information you receive:

- Comes from the person who is named on the envelope or header?
- Is exactly the same as it was when it was sent?
- Has not been copied by anyone during transit?

Are you equally certain that the information you send is delivered to the intended receiver (and to no one else)?

The simple answer is no, unless you hand deliver all of your documents. Post, fax and email are subject to forgery, alteration, being revealed to outsiders, and uncertainty about delivery. The paper world is more trusted than email because of certain measures that can be taken: signatures and signature matching, sealed envelopes, trusted couriers, and signing upon receipt of a document. Of course, these paper trails are expensive and error prone.

Digital security, however, can provide the ease of use and speed of email – along with superior security and audit trails over the paper world.

bolero.net has implemented a digital security system that ensures:

- Authenticity of the identity of the sender of a message.
- That if a message has been altered in any way, it will be rejected from the system.
- Confidentiality through encryption.

How does digital security work in the bolero.net system?

The Old Way

Until recently, when two parties wanted to secure their communication over a network, such as the Internet, they had to exchange a secret key, much like a sophisticated password. You gave your password to your partner, and she gave hers to you. Whenever you wanted to send something to her, you locked the message with her password. When she received it, she entered her password and could access the message. If anyone else received it, they would not know the password and could not open the message.

While this system did provide good security, it had a number of drawbacks. One significant drawback is that you could only send secret messages to the person who had the key. The other difficulty is that you had to exchange this key in a most secure way: probably in person. That is hardly the way to create an electronic trade community.

The bolero.net system's way

To counter the downsides, public key infrastructure (PKI) was designed. A PKI system uses two keys – a secret or private key and a public key – instead of one. The private key never leaves its owner, while the public key is made available to everyone.

Both keys are created at the same time through a complex mathematical computation. The private key is stored on a portable, secure media, such as a workstation.

The method to create the keys uniquely links the keys together such that the public key can be used to verify the private key, but you will be unable to calculate the private key by knowing the public key.

Digital security in bolero.net works in three ways:

- Secure Socket Layer (SSL) connections between Users and the bolero.net system

- Digital signatures
- Encryption

SSL

SSL is the standard protocol for establishing secure connections between two parties in an open network environment, such as the Internet. When you log onto the bolero.net system's web services, your communication is confidential: no one can understand the information you are exchanging. And it is also authenticated, meaning that you are certain that you're talking to Bolero and Bolero is certain that it is talking to you.

Digital Signatures

A digital signature is created by applying the private key of the sender to the message he is sending. The receiver of the message uses the sender's public key to verify the digital signature. All messages must be signed in order to be accepted by the bolero.net system.

Digital signature verification demonstrates that:

- 1 The digitally signed message has not been altered since it was digitally signed. (This process is discussed later.)
- 2 The digital signature has been created with the private key corresponding to the public key that is listed in the certificate. The certificate identifies the sender. The recipient's computer can thus infer (based on mathematical relationships between the key pairs) that a particular user of bolero.net created the digital signature.

Since all Bolero messages are verified by bolero.net before being forwarded to the intended recipient, the recipient verifies the bolero.net digital signature when downloading a message. The table below illustrates the process. The numerals indicate the order of the actions.

| | User's computer | bolero.net System | Receiver's computer |
|----------------------|----------------------|----------------------|---------------------|
| Signs with | 1 User's private key | 3 Bolero private key | - |
| Verifies with | - | 2 User's public key | 4 Bolero public key |

If the message was altered – even by as much as one character – along the way, the message will be halted, and the sender will be notified.

Encryption

Messages can be encrypted if their contents need maximum secrecy during delivery (subject to the laws in your jurisdiction). If anyone somehow manages to intercept an encrypted message, it will be unreadable.

Encryption in bolero.net utilizes the key pairs, but in a different way than they are used for digital signatures. The sender uses the receiver's public key to encrypt. Since the receiver's private key is needed to decrypt the message, no one but the receiver can ever see the contents.

The following table demonstrates the process.

| | User's computer | bolero.net | Receiver's computer |
|----------------------|---------------------------|----------------------------|----------------------------|
| Encrypts with | 1 bolero.net's public key | 3 Receiver's public key | - |
| Decrypts with | - | 2 bolero.net's private key | 4 Receiver's private key |

How to get certified

A company must go through the entire enrolment process to become digital-security enabled for the Bolero System. This section explains the technical part of the enrolment process. Following is the procedure a company must complete. From an operative perspective, this takes very little time.

Make the Initial Decisions

Before proceeding, please read the downloadable document *User Identifiers Explained*.

Select a User Identifier

The Root Registered Identifier (“Root RID”) is required during the enrolment process. Bolero permits a User to select its Root RID, as long as certain rules are observed. If a Root RID is unacceptable, the applicant will be notified and will have to select another. Refer to the Bolero *Operating Rules* for details.

Decide Whether to Have Separate Security Administrator Role

A User has the option to divide administrative responsibilities into two roles. The required role is the Business Administrator, but there can be an option Security Administrator role, as well. At the very beginning of the process to get digital-security enabled, you need to decide whether to have one or two roles. If you want choose two roles, you will need to generate two key pairs and certificate requests.

If there will be a Security Administrator, the responsibilities will be split according to the diagram below. Otherwise, the Business Administrator assumes all responsibilities.

| <i>Business Administrator</i> | <i>Security Administrator</i> |
|--|--|
| Set up Sub-accounts. | Generate security keys. |
| Manage Sub-accounts. | Obtain certificates from the Bolero Certification Authority. |
| Update Sub-accounts. | Store keys and certificates in appropriate hardware devices (i.e., smart cards). |
| Remove Sub-accounts. | Associate certificates to RIDs and functions. |
| Mailbox management. | Remove certificates from the Bolero System. |
| Management and control, including local reporting, logging and verification. | Certain management and control functions. |

Prepare for Certification

Generate a Key Pair and Certificate Request

The administrator generates a PKCS#10 certificate request and a public/private key pair. Bolero-enabled software makes this procedure simple from an operational perspective. In fact, it takes just a few minutes. Depending on what software product you use, the process will vary. Following is a general description of the process.

Security Procedures

The key generation creates the key that is used for digital signatures. It must be kept securely from the moment of generation, because you do not want others to be able to impersonate you by using your digital signature. Therefore, the key generation process should be conducted in a secure environment and with possible other control measures. You should consider

the trustworthiness of the workstation you use for key generation, where the private key resides from the moment of generation, who has access to it, firewall protection, virus-checking, etc.

There are publicly available procedures – many of which are available through the Internet – that provide suggestions for this process.

Note that there are specific operating rules in the *Operating Procedures* that pertain to security, including rules 1 through 4.

Generating the Key Pair and Certificate Request

You generate a key pair through whatever Bolero software you have chosen. The following terms may differ depending on the interface that you are using.

Select the option to generate new keys and certificates. You will have to give a Common Name to the keys. The following convention must be used:

- If single authorisation is selected, use the RootID.
- If dual authorisation is selected, use Root RID:ba and Root RID:sa.

You might need to enter a temporary PIN during the key generation process. This PIN will be used when you receive your certificate from bolero.net and complete the process. If a PIN is required, please make a note of it and keep it securely.

You will then be prompted to select a filename and location to save the PKCS#10 certificate request. Please use the following convention to save the PKCS#10 file:

[Root RID].PKCS10 (if you chose the single authorisation option)

or

[Root RID].BA.PKCS10 (if you chose the dual authorisation option)

If you chose the single authorisation option, you have now completed the key generation and certificate request process. If you chose the dual

authorisation option, you will need to repeat the process for the security administrator key pair and certificate request.

Please use the following convention to save the PKCS#10 file of the security administrator:

[Root RID].SA.PKCS10

You can now send the one or two PKCS10 files that you have just created to the following email address:

enrolment@bolero.net

Providing the Certificate Request in the BIL Application Form

Bolero International will need to verify your electronic certificate request against a documentary (paper) version. To provide the documentary version, open the PKCS10 file (the “RootID.BA.PKCS10” file if dual authorisation is chosen) using a text editor such as Microsoft Notepad.

[NOTE: Do not use a word processing programme such as Microsoft Word for this process].

Next, select all of the text, and copy and paste it into the Bolero International Limited application form. The text will be similar to this:

```
-----BEGIN CERTIFICATE REQUEST-----  
IIBkDCB+/2t48dad1BkWWVNV5likCf8hOybZDf0uVKakIXhVMSQCruqhNuon1gcKjk  
hBB75JyYLoJQCjHouoGN6cyYENV5likCf8hOybZDf0uVKakIXNV5likCf8hOybZDf0  
IIBkDCB+/2t48dad1BkWWVNV5likCf8hOybZDf0uVKakIXhVMSQCruqhNuon1gcKjk  
hBB75JyYLoJQCjHouoGN6cyYENV5likCf8hOybZDf0uVKakIXNV5likCf8hOybZDf0  
uVKakIXv557wAIIBkDCB+/2t48dad1BkWWVNV5likCf8hOybZDf0uVKakIXhVMSQCr  
uNuon1gcKjkhBB75JyYLoJQCjHouoGN6cyYENV5likCf8hOybZDf0uVKakIXNV5lik  
Cf8hOybZDf0uVKakIXv557wAIIBkDCB+/2t48dad1BkWWVNV5likCf8hOybZDf0uVK  
akIXhVMSQCruNuon1gcKjkhBB75JyYLoJQCjHouoGN6cyYENV5likCf8hOybZDf0uV  
-----END CERTIFICATE REQUEST-----
```

If you requested dual authorisation, you will now need to repeat the process with the “Root RID.SA.PKCS10” file.

You have now completed the certification part of the enrolment process. You will need to complete all other steps that are required as part of the process before returning the enrolment packs to the Bolero Association.

Complete Certification

Import Certificate

When the Bolero Association and Bolero International have finished verifying your materials, Bolero International will complete the certification process and will send your certificate(s) to the Primary Representative.

You will now need to import the certificate(s) into your environment. Save the certificates according to the instructions provided with your Bolero interface.

Since you will be importing the certificate to a smart card, you will have to enter a smart card into the reader. If you used a PIN during the key generation and certificate request process, you will need to use the PIN to access the private key.

You will now need to import the certificate into your environment using the file commands in your Bolero software.

You have now completed the certification process. You are ready to begin user creation and certificate assignment through the Bolero interactive services.