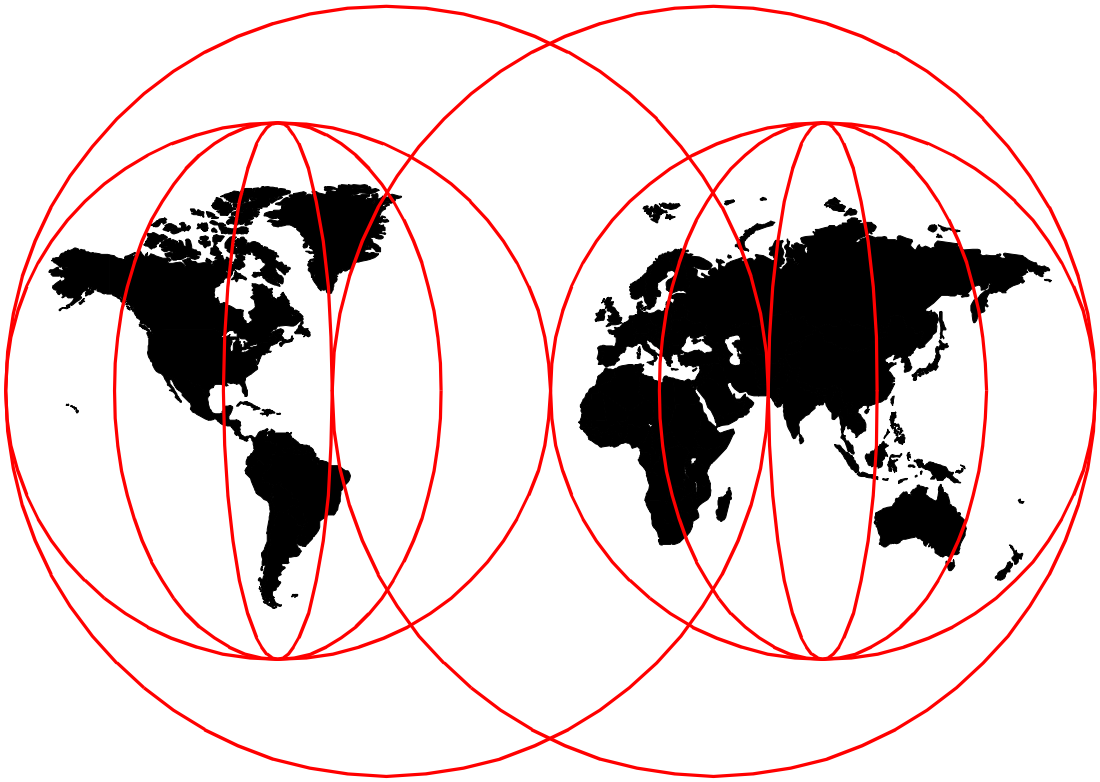
Global Server Certificate Usage with OS/390 Webservers

Paul de Graaff, Ulrich Boche



International Technical Support Organization

http://www.redbooks.ibm.com

SG24-5623-00

International Technical Support Organization

SG24-5623-00

Global Server Certificate Usage with OS/390 Webservers

May 1999

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix C, “Special Notices” on page 41.

First Edition (May 1999)

This edition applies to Domino Go Webserver Release 5.0, Program Number 5697-D43 for use with OS/390 Version 2 Release 5 or later.

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. HYJ Mail Station P099
522 South Road
Poughkeepsie, NY 12601-5400

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© Copyright International Business Machines Corporation 1999. All rights reserved.
Note to U.S Government Users - Documentation related to restricted rights - Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Contents

© Copyright IBM Corp. 1999

Figures

© Copyright IBM Corp. 1999

Preface

This redbook gives a broad understanding of the use of so called Global Server Certificates in Domino Go Webserver Release 5.0 and upwards on OS/390 version 2 Release 5.

It contains an introduction to Digital Certificates and Secured Sockets Layer (SSL). That will be especially useful for people just starting to use digital certificates and want to understand their use with Web servers and Web browsers.

It also contains detailed information on requesting and implementing Global Server Certificates into their OS/390 Webserver. This will be especially useful for system programmers and security personnel who need to exploit this technology.

The Team That Wrote This Redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization Poughkeepsie Center.

Paul de Graaff was the project leader. He is a Certified IT Specialist at the International Technical Support Organization, Poughkeepsie Center. He writes extensively and teaches IBM classes worldwide on all areas of S/390 Security. Before joining the ITSO, Paul worked with IBM Global Services in The Netherlands as a senior IT Specialist.

Ulrich Boche is an IT Technical Consultant in Germany. He has 27 years of experience in IBM Large Systems software. His areas of expertise include RACF, cryptography, DCE and security in an open, networked computing environment. He has written extensively on Large Systems security topics.

Thanks to the following people for their invaluable contributions to this project:

Richard Conway
International Technical Support Organization, Poughkeepsie Center

Terry Barthel
International Technical Support Organization, Poughkeepsie Center

Carol Dixon
International Technical Support Organization, Poughkeepsie Center

Blake Carlson
VeriSign Inc.

Eric Denton
VeriSign Inc.

Comments Welcome

Your comments are important to us!

© Copyright IBM Corp. 1999

We want our redbooks to be as helpful as possible. Please send us your comments about this or other redbooks in one of the following ways:

- Fax the evaluation form found in “ITSO Redbook Evaluation” on page 49 to the fax number shown on the form.
- Use the online evaluation form found at `http://www.redbooks.ibm.com`
- Send your comments in an Internet note to `redbook@us.ibm.com`

Chapter 1. Introduction to Digital Certificates and SSL

The intent of this chapter is to provide a basic understanding of the use of digital certificates in Web applications and Secure Sockets Layer (SSL).

1.1 Digital Certificates

The application of public-key technology requires that the use of a public key be confident that such a public key received over a communications channel really belongs to the sender, with the remote person or system being the partner in the use of an encryption or digital signature mechanism. This confidence is obtained through the use of public-key certificates. A *digital certificate* is analogous to a passport: the passport certifies the bearer's identity, address and citizenship. The concepts behind passports and other identification documents like, drivers licenses, are very similar to those used for digital certificates.

For example, identification documents are issued by a trusted authority, such as the Government passport office or the Department of Motor Vehicles. A passport will not be issued unless the person who requests it has proven his or her identity and citizenship to the authority. Specialized equipment is used in the creation of passports to make it very difficult to alter the information in it or to forge a passport altogether. Other authorities, for instance the border police in other countries, can verify a passport's authenticity. If they trust the authority that issued the document, the information contained in it will be accepted as true.

Simirlarly, a digital certificate serves two purposes: it establishes the owner's identity and it makes the owner's public key available. Like a passport, a certificate must be issued by a trusted authority, a *certification authority (CA)* and, also like a passport, it is issued only for a limited time. When its expiration date has passed, it must be replaced.

The information about the certificate owner's identity is stored in a format that follows the X.500 standard, for instance: cn="Ulrich Boche", o="IBM Corporation", and so on; the complete information is called the owner's *Distinguished Name (DN)*. The owner's distinguished name and public key are digitally signed by the certificate authority; that is, a message digest (MIC) is calculated from the DN and the public key and the MIC are encrypted with the private key of the certification authority. Figure 1 on page 2 shows a simplified layout of a digital certificate.

© Copyright IBM Corp. 1999

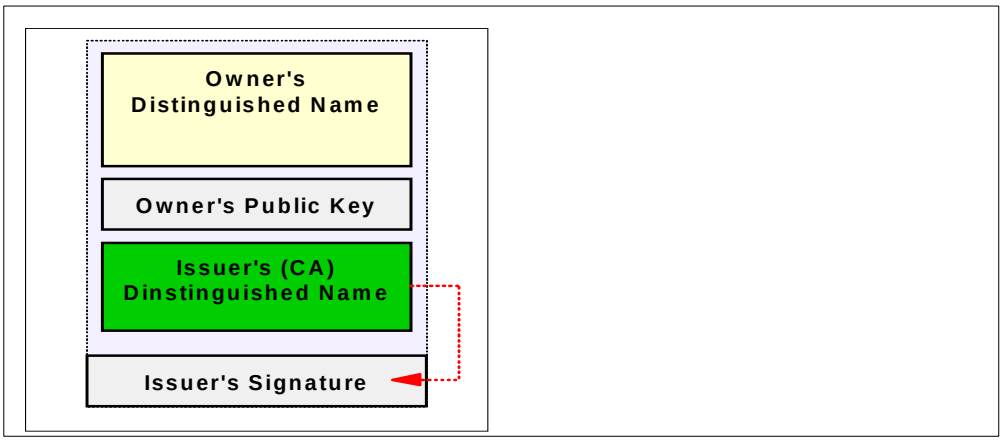


Figure 1. Digital Certificate - Simplified Layout of an X.509 Digital Certificate

The digital signature of the certification authority serves the same purpose as the special measures taken for the security of passports such as, for example, laminating pages with plastic material: it allows others to verify the authenticity of the certificate. Using the public key of the certification authority, the MIC can be decrypted. The message digest can be recreated; if it is identical to the decrypted MIC, the certificate is assumed to be authentic.

Trust is a very important concept in passports as well as in digital certificates. In the same way as, for instance, a passport issued by some governments, even if recognized to be authentic, will probably not be trusted by US authorities, so each organization or user has to determine which certification authorities can be accepted as trustworthy.

1.1.1 Security Considerations for Certificates

You may ask, if I send my certificate with my public key in it to someone else, what keeps this person from misusing my certificate and posing as me? The answer is: your private key.

A certificate alone can never be proof of anyone's identity. The certificate just allows you to verify the identity of the certificate owner by providing the public key that is needed to check the certificate owner's digital signature. Therefore, the certificate owner must protect the private key that belongs to the public key in the certificate. If the private key is stolen, the thief can pose as the legitimate owner of the certificate. Without the private key, a certificate cannot be misused.

An application that authenticates the owner of a certificate cannot accept just the certificate. A message signed by the certificate owner should accompany the certificate. This message should use elements such as sequence numbers, time stamps, challenge-response protocols or other data that allow the authenticating application to verify that the message is a “fresh” signature from the certificate owner, and not a replayed message from an imposter.

1.1.2 Certification Authorities and Trust Hierarchies

A user of a security service requiring knowledge of a public key generally needs to obtain and validate a certificate containing the required public key. Receiving a certificate from a remote party does not give the receiver any assurance about

the authenticity of the certificate. To verify that the certificate is authentic, the receiver needs the public key of the certification authority that issued the certificate.

If the public-key user does not already hold an assured copy of the public key of the certification authority that signed the certificate, then it might need an additional certificate to obtain that public key. In general, a chain of multiple certificates may be needed, comprising a certificate of the public key owner (the end entity) signed by one CA, and zero or more additional certificates of CAs signed by other CAs. Figure 2 shows a chain of trust.

Many applications that send a subject's certificate to a receiver not only send just that certificate, but also all the CA certificates necessary to verify the certificate up to the root.

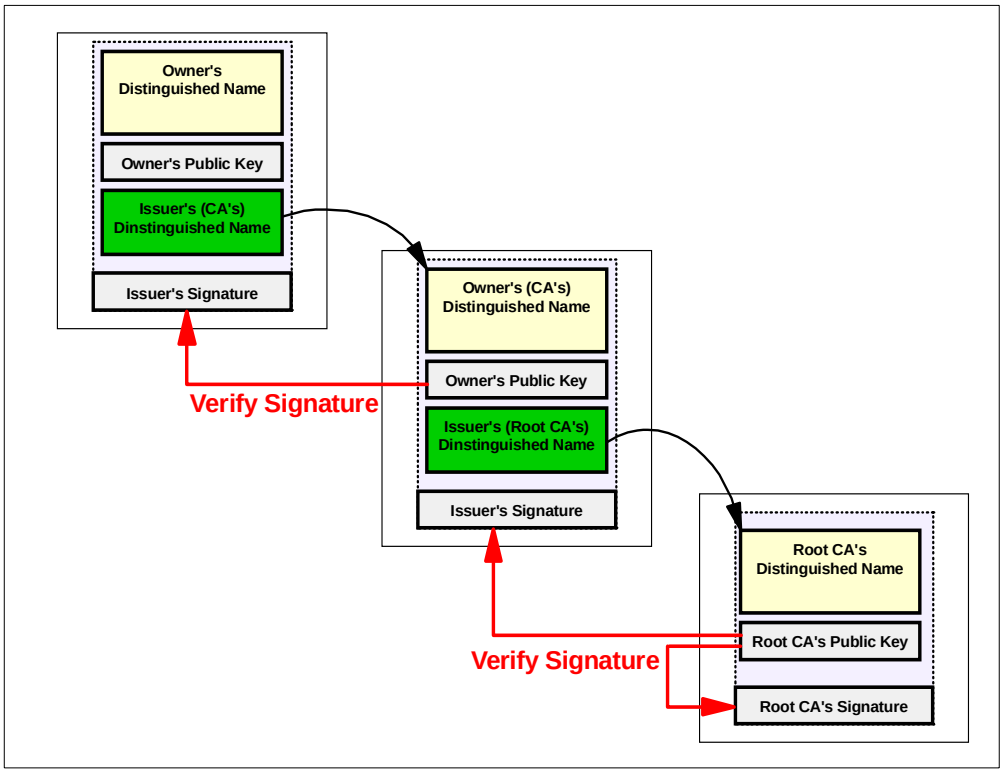


Figure 2. Chain of Trust - CAs Signing CA Certificates up to the Root CA

The chain of trust begins at the root CA. The root CA's certificate is self-signed, that is, the certification authority used its own private key to sign the certificate. The public key used to verify the signature is the public key in the certificate itself (see Figure 3 on page 4). To establish a chain of trust, the public-key user must have received the certificate of the root CA in a trustworthy manner.

This could be done in different ways, for example, on a diskette received by registered mail or picked up in person, or pre-loaded with software received from a reliable source or downloaded from an authenticated server.

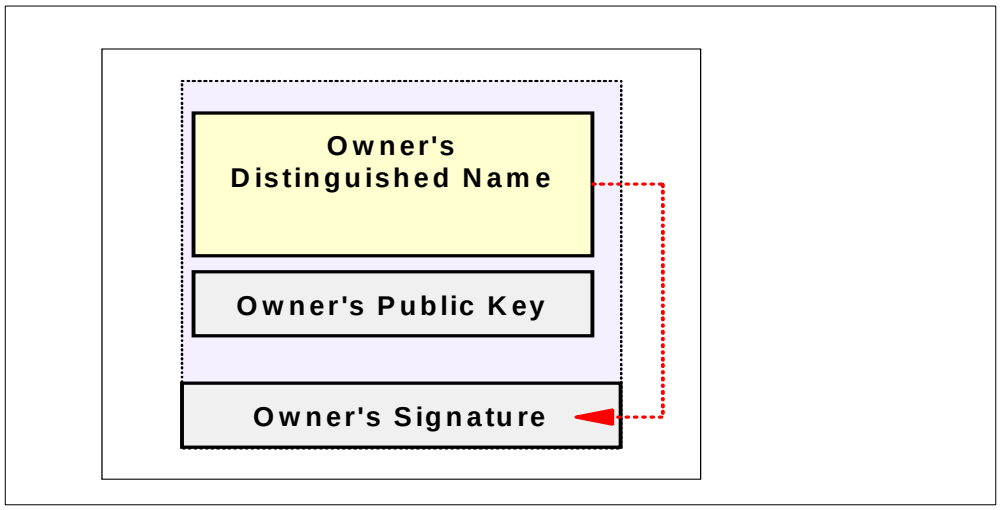


Figure 3. Self-Signed Certificate - Signed with Certificate Owner's Private Key

1.1.2.1 Public Key Infrastructure (PKI)

A Public Key Infrastructure (PKI) defines the rules and relationships for certificates and certification authorities in a certain environment. It defines the fields that can or must be in a certificate, the requirements and constraints for certification authorities in issuing certificates, whether there can be only one root CA or multiple, and how certificate revocation is handled. A number of Public Key Infrastructures have been defined and more will certainly follow. Some of them are listed here.

Privacy Enhanced Mail (PEM): This PKI, defined in RFC 1422, was created for secure e-mail exchange in the Internet using PEM and is based on X.509 V.1 certificates. It defines a rigid architecture of CAs with one root, the Internet Policy Registration Authority (IPRA). The IPRA only issues and signs the certificates of the second-level CAs, the Policy Certification Authorities (PCAs). These in turn issue and sign the certificates of certification authorities, at level three, which issue user certificates and certificates for lower-level CAs.

A PCA must establish and publish a statement of its policy with respect to certifying users or subordinate certification authorities. Distinct PCAs aim to satisfy different user needs. For example, one PCA (an organizational PCA) might support the general electronic mail needs of commercial organizations, and another PCA (a high-assurance PCA) might have a more stringent policy designed for satisfying legally binding signature requirements.

Secure Electronic Transaction (SET): SET is a secure payment protocol for the Internet based on credit cards. It is endorsed by VISA and MasterCard. The certificates used in SET are X.509 V.3 with non-standard extensions. Its PKI defines a single root CA who signs the certificates of the VISA and MasterCard organizations. This root CA is a company named SETCo, founded by both VISA and MasterCard. However, some SET products (like those from IBM) also support so-called *private brand CAs*, that is, root CAs outside the SET root.

The certificates of issuer bank CAs (issuers of credit card certificates to cardholders) and acquirer bank CAs (issuers of certificates to merchants) are signed by VISA and MasterCard.

Internet Public Key Infrastructure (IPKI): This PKI which is based on X.509 V.3 certificates is currently a draft by the PKIX working group for the IETF. Its goal is to develop a profile and associated management structure to facilitate the adoption/use of X.509 certificates within Internet applications for those communities wishing to make use of X.509 technology. Such applications may include WWW, electronic mail, user authentication, and IPSEC, as well as others.

IPKI does not require a single root CA. Multiple domains may exist with their own root CA which provides advantages for many environments, especially in Intranet and Extranet situations.

Other Public Key Infrastructures: Lightweight Directory Access Protocol (LDAP) directories can be used to store certificates. They can provide a secure, centralized repository for user and certification authority certificates, making it easier to establish trust. They are also especially useful to store certification revocation information (see the following item).

Certificate Revocation: An important part of any Public Key Infrastructure is the handling of certificate revocation. Certificates can become invalid for different reasons, such as the following:

- The computer that holds the certificate owner's private key may get stolen.
- The private key of the certificate owner may get compromised.
- For certificates such as in SET, the credit card of the owner of the certificate may get revoked (for example, due to bad credit).
- For certificates issued by a corporation or organization, the owner of the certificate may no longer be part of the corporation or organization.

Without proper means for handling revoked certificates, a certificate can be used until its expiration date has been reached. In an environment where this is not acceptable, ways must be found and implemented to make certificate revocation known to those who base actions upon verified certificates.

In some Public Key Infrastructures, *Certificate Revocation Lists (CRLs)* have been implemented. A CRL has information about certificates that are no longer valid. Since CRLs must either be downloaded from a CRL server (pull method) or automatically distributed to receivers (push method), the implementation is not without problems. Public Key Infrastructures with LDAP directories are expected to provide significant improvements in this area.

1.1.3 Uses for Certificates in Internet Applications

Applications using public-key cryptosystems for key exchange or digital signatures need to use certificates to obtain the needed public keys. Internet applications of this kind are quite numerous and we will briefly discuss just a few important ones:

- Secure Sockets Layer (SSL)

  SSL, a protocol that provides privacy and integrity for communications, is used today by Web servers for secure connections between Web servers and Web browsers, by the Lightweight Directory Access Protocol (LDAP) for secure connections between LDAP clients and LDAP servers, and by Host-on-Demand V.2 for connections between the client and the host system. More applications will follow.

SSL uses certificates for key exchange, server authentication and, optionally, client authentication. See 6.5, "Secure Sockets Layer (SSL)" for a more detailed description of SSL.

- Client Authentication

  Domino Go Webserver on OS/390 has the ability to cooperate with RACF. Users can be authenticated by RACF and their access authorities to data (HFS files or MVS data sets), IMS or CICS transactions, or DB2 tables and views can be dependent on their RACF identities.

  Previously, this required the user to be authenticated by RACF user ID and password. Domino Go Webserver 4.6.1, together with OS/390 Security Server (RACF) V2R5, can use the client certificate from SSL client authentication to obtain the client's user ID from RACF and use it for all of this client's requests. This requires the user's client certificate and user ID to be associated in RACF, for example with the RACF command RACDCERT.

- Secure Electronic Mail

  Many electronic mail systems, using standards such as PEM or S/MIME for secure electronic mail, use certificates for digital signatures and for the exchange of keys to encrypt and decrypt messages.

- Virtual Private Networks (VPN)

  Virtual Private Networks, also called *secure tunnels*, can be set up between firewalls to enable protected connections between secure networks over insecure communication links. All traffic destined to these networks is encrypted between the firewalls.

  The protocols used in tunneling follow the IPsec standard. For the key exchange between partner firewalls, the *Internet Key Exchange (IKE)* standard, previously known as ISAKMP/Oakley, has been defined.

  The standards also allow for a secure, encrypted connection between a remote client (for example, an employee working from home) and a secure host or network.

- Secure Electronic Transaction (SET)

  SET is a standard designed for secure credit card payments in insecure networks (the Internet). Certificates are used for cardholders (“electronic credit cards”) and merchants. The use of certificates in SET allows for secure, private connections between cardholders, merchants and banks. The transactions created are secure, indisputable and unforgeable. The merchants receive no credit card information that could be misused or stolen.

1.1.3.1 Formats and Standards for Certificates

The standard known as ITU-T X.509 (formerly CCITT X.509) or ISO/IEC 9594-8, which was first published in 1988 as part of the X.500 Directory recommendations, defines a standard certificate format. ITU means International Telecommunication Union, an organization of worldwide telecommunications companies (originally the national telephone companies). The standard has been extended twice, the current version is X.509 Version 3. The X.509 V.3 certificate standard is generally accepted today.

Unfortunately, this does not necessarily mean that everybody can handle everybody else's certificates without any problem. The standard defines extensions which are not necessarily implemented everywhere.

Commonly, an X.509 V.3 certificate has at least the following fields:

- Version
- Serial number
- Signature algorithm ID
- Issuer distinguished name
- Validity period
- Subject (owner) distinguished name
- Subject public key
- Issuer unique identifier
- Subject unique identifier
- Extensions
- Signature on the above fields

Also, when certificates are transferred, different formats can be used that can lead to communications problems. Some of the more frequently used formats in the following sections. Note that the internal representation of certificate fields are described in some of the formats differ, as different encoding methods are used.

1.1.3.2 PEM Certificate Format

The PEM format, specified in RFC 1422, can be used both for certificate requests and for signed certificates. This format is supported by the utilities MKKF and CERTUTIL of Domino Go Webserver 4.6.1 for OS/390.

1.1.3.3 PKCS #7 Certificate Format

The PKCS #7 format can be used for signed certificates only, but not for certificate requests. This format is supported by a number of products. Certificates downloaded in PKCS #7 format and copied into an MVS data set (in binary, without ASCII/EBCDIC conversion) can be used by the RACF command RACDCERT.

1.1.3.4 PKCS #10 Certificate Format

The PKCS #10 format is used for certificate requests only, it cannot be used for signed certificates. It was created to allow for a certificate request format with a minimum of data to be transferred.

1.1.3.5 PKCS #12 Certificate Format

The Web browsers Netscape Navigator and Communicator and Microsoft Internet Explorer are using the PKCS #12 format to transfer certificates. This format is also used to export and import certificates (including the private key). In this case, the exported file is encrypted with a key that is derived from a user-specified password.

A certificate can only be transferred into another Web browser or onto another PC when the private key is moved with the certificate. Exporting the certificate and private key to a PKCS #12 file and importing them at the other location is the only way we know of to perform this task.

Attention

The specifications for all PKCS standards can be downloaded from the Web site of RSA Data Security Inc., at:

`http://www.rsa.com`

1.1.3.6 Certificates and Certificate Requests

Simplified, a signed certificate contains the owner's distinguished name, the owner's public key, the certification authority's (issuer's) distinguished name and the signature of the certification authority over these fields (see Figure 1 on page 2).

A self-signed certificate (a root CA certificate) contains the owner's distinguished name, the owner's public key, and the owner's own signature over these fields (see Figure 3 on page 4).

A certificate request that is sent to a certification authority to be signed contains the owner's (requester's) distinguished name, the owner's public key, and the owner's own signature over these fields. The certification authority verifies this signature with the public key in the certificate in order to make sure that:

1. The certificate request was not modified in transit between the requester and the CA.
2. The requester is in possession of the private key that belongs to the public key in the certificate request.

Comparing the contents of a self-signed certificate and a certificate request, it is obvious that, for all practical purposes, these two types are identical.

1.2 Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) is a protocol that provides privacy and integrity between two communicating applications using TCP/IP. The HyperText Transfer Protocol (HTTP) for the World Wide Web uses SSL for secure communications.

The data going back and forth between client and server is encrypted using a symmetric algorithm such as DES or RC4. A public-key algorithm, usually RSA, is used for the exchange of the encryption keys and for digital signatures. For this purpose, the public key in the server's certificate is used. With the server certificate, the client is also able to verify the server's identity. Versions 1 and 2 of the SSL protocol only provided for server authentication. With SSL Version 3, the possibility of authenticating the client identity by using client certificates in addition to server certificates was added.

A Secure Sockets Layer connection is always initiated by the client by using an URL starting with https:// instead of http://. At the beginning of an SSL session, an SSL handshake is performed. This handshake produces the cryptographic parameters of the session. A simplified overview of the SSL handshake is shown in Figure 4 on page 9.

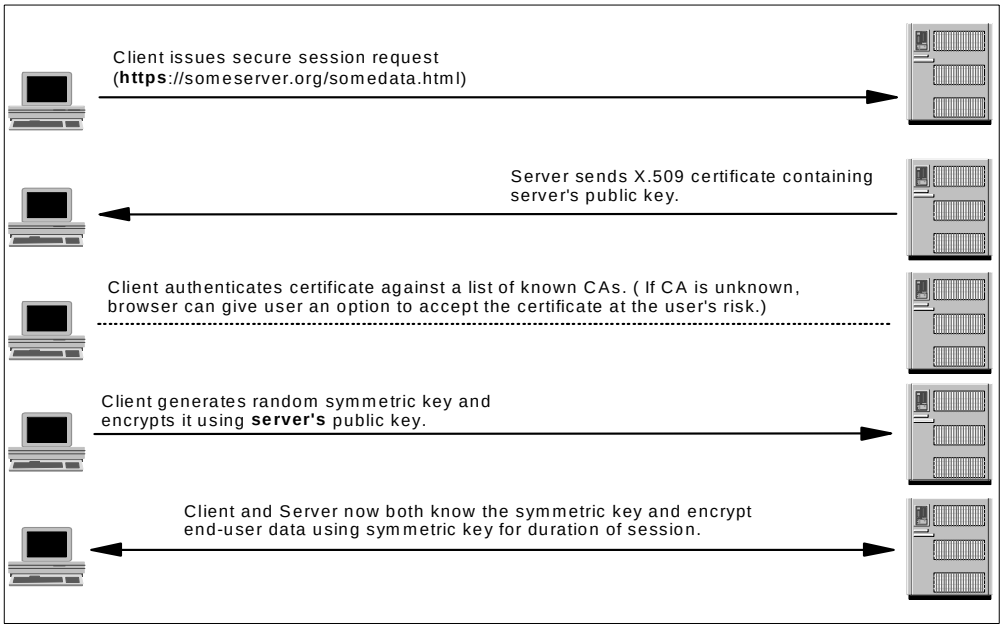


Figure 4. SSL Handshake - SSL V.2 Handshake with Server Authentication

This figure illustrates the following sequence:

1. First, the client sends a client hello message which lists the cryptographic capabilities of the client (sorted in client preference order) and contains a 28-byte random number.
2. The server responds with a server hello message which contains the cryptographic method (cipher suite) selected by the server, the session ID and another random number.

> **Important**
>
> Client and server must support at least one common cipher suite or the handshake will fail.

3. Following the server hello message, the server sends its certificate. With Secure Sockets Layer, X.509 V.3 certificates are used.
4. Following the server hello message, the server sends its certificate. With Secure Sockets Layer, X.509 V.3 certificates are used.
5. If SSL Version 3 is used and the server application (for example, the Web server) requires a certificate for client authentication, the server sends a certificate request message. In the certificate request message, the server sends a list of the types of certificates supported and the distinguished names of acceptable certification authorities.
6. The server then sends a server hello done message and waits for a client response.
7. Upon receipt of the server hello done message, the client (the Web browser) verifies the validity of the server's certificate and checks that the server hello parameters are acceptable.

8. If the server requested a client certificate, the client sends a certificate or, if no suitable certificate is available, a no certificate alert. This alert is only a warning, but the server application can fail the session if client authentication is mandatory.
9. The client then sends a client key exchange message. This message contains the so-called pre-master secret, a 46-byte random number which will be used in the generation of the symmetric encryption keys and the Message Authentication Code (MAC) keys, encrypted with the public key of the server.
10. If the client sent a certificate to the server, the client will now send a certificate verify message which is signed with the client's private key. By verifying the signature of this message, the server can explicitly verify the ownership of the client certificate.

> **Attention**
>
> A similar process to verify the server certificate is not necessary. If the server does not have the private key that belongs to the certificate, it cannot decrypt the pre-master secret and create the correct keys for the symmetric encryption algorithm, and the handshake must fail.

11. Now the client uses a series of cryptographic operations to convert the pre-master secret into a master secret, from which all key material required for encryption and message authentication is derived. Then, the client sends a change cipher spec message to make the server switch to the newly negotiated cipher suite.
12. The finished message which immediately follows is the first message encrypted with this cipher method and keys.
13. After the server responds with a change cipher spec and a finished message of its own, the SSL handshake is complete and encrypted application data can be sent.

1.2.1 Certificates and Trust Chains with SSL

Secure Sockets Layer V.3 can use server certificates as well as client certificates. As we have seen, server certificates are mandatory for an SSL session while client certificates are optional, depending on client authentication requirements.

The Public Key Infrastructure used by SSL allows for any number of root certification authorities. An organization or end user must decide for themselves which CAs they will accept as trusted. To be able to verify the server certificates, client Web browsers need to be in possession of the root CA certificates used by servers. Popular Web browsers such as Netscape Navigator or Communicator or Microsoft Internet Explorer usually come with a key ring where a number of CA certificates, so-called *trusted roots*, are already installed. It is usually possible to edit this list and delete the certificates of untrusted CAs.

If an SSL session is about to be established with a server that sends a certificate whose root CA certificate is not in the key ring, the browser will display a warning window and present options to either import the certificate or abort the session. To avoid this situation, it can be desirable to import the root CA certificate from a Web page (for a description, see 8.1.5, "Distributing the Self-Signed CA

Certificate to the Browsers") or to use a JavaScript program that imports the certificate.

If client authentication is used, the Web server needs to be in possession of the root CA certificates used by clients. Since it is not possible to dynamically import root CA certificates into the OS/390 Domino Go Webserver, all root CA certificates that are not part of the server key ring at delivery time must be installed using the MKKF utility before any client certificates are issued by these certification authorities.

Chapter 2. Global Server Certificates

In this chapter, we discuss Global Server Certificates, a special kind of server certificate for Web servers.

2.1 The Need for Global Server Certificates

To understand why Global Server Certificates are needed, we have to look at the restrictions on export of cryptographic hardware and software imposed by the US Government.

- Users in the United States and Canada can use any available cryptographic algorithm with any key length. Delivery of cryptographic hardware and software to customers in the US and Canada is unrestricted.
- Users in other countries may only use cryptographic algorithms up to certain key lengths. Delivery of cryptographic hardware and software to customers outside the US and Canada is restricted and controlled by the US Government.

The US Government export regulations allow certain industries in countries outside the United States and Canada (currently financial institutions such as banks and insurance companies and health industry organizations) to use cryptographic products with the same key lengths as in the United States.

To be able to use these strong encryption algorithms, eligible customers must order and use US versions of cryptographic products such as the OS/390 Web server. However, in the SSL environment, this alone is insufficient since both the client and the server must agree on a cryptographic protocol they both can support.

As opposed to US versions of Web servers, the US Government does not allow the export of US versions of Web browsers such as Netscape Communicator or Microsoft Internet Explorer to end users outside the United States and Canada at all. This means that every Web browser exported by Netscape or Microsoft can only have the capability to do RC4 or RC2 encryption with key lengths of 40 bits. Therefore, ways had to be found to enable these Web browsers to use strong cryptographic algorithms only in sessions with Web servers authorized by the US Government for strong encryption.

To solve this problem, Global Server Certificates were created. The US Government has authorized VeriSign, Inc. to issue special server certificates to customers eligible to use strong encryption, such as banks and other financial institutions, insurance companies, and health industry organizations. These certificates are recognized by Microsoft Internet Explorer Version 3.02 and up and by Netscape Navigator/Communicator Version 4 and up. When the WebWeb browser recognizes the special certificate, it enables strong encryption routines such as RC4 with 128-bit keys or Triple DES with 168-bit keys. This process is sometimes also called *Server Gated Cryptography (SGC)*.

2.1.1 Who needs Global Server Certificates

Global Server Certificates are needed by:

© Copyright IBM Corp. 1999

- Banks, financial institutions, insurance companies, health care organizations outside the United States and Canada who need to use Secure Sockets Layer (SSL) between their Web servers and their customers' and users' Web browsers with encryption stronger than RC2 or RC4 with 40-bit keys.
- Banks, financial institutions, insurance companies, health care organizations inside the United States or Canada who need to use Secure Sockets Layer (SSL) between their Web servers and the Web browsers of customers or users located outside the US or Canada with encryption stronger than RC2 or RC4 with 40-bit keys.

2.2 Installing Global Server Certificates

Before a Global Server Certificate can be installed in Domino Go Web Server 5.0, it has to be requested and received from VeriSign Inc.

Important

Only Domino Go Webserver Release 5.0 for OS/390 and later releases are able to work with Global Server Certificates. Prior releases of DGWS or Internet Connection Secure Server cannot support this type of certificate.

In this section, we first describe how to request a Global Server Certificate from Verisign Inc. and then how to install the certificate in DGWS 5.0.

For details on how to use the IKEYMAN utility, refer to *Domino Go Webserver Webmaster's Guide Rel. 5 for OS/390*, SC31-8691or *Enterprise Web Serving with the Lotus Domino Go WebServer for OS/390*, SG24-2074.

2.2.1 Requesting a Global Server Certificate

Like all other client and server certificates, Global Server Certificates can be requested and received over the Internet. The procedure involves creating a certificate request file with the DGWS 5.0 key management utility and sending the request to VeriSign Inc.

Before starting with the certificate request creation, you should have the following items available:

1. A so-called D-U-N-S number from Dun & Bradstreet. Dun & Bradstreet is a company that provides information for investors worldwide and D-U-N-S stands for *Data Universal Numbering System*. It is a company identifier in Electronic Data Interchange (EDI) and global electronic commerce transactions. VeriSign Inc. relies on D-U-N-S numbers to identify the companies and determine their entitlement to a Global Server Certificate. If your company does not have a D-U-N-S number yet, now is as good a time as any to get one since having this number will speed up processing of your certificate request quite considerably. For the Dun & Bradstreet office in your country, see the list in Appendix A, "Dun & Bradstreet Offices" on page 39 or check:
   `http://www.dnb.com/global/menu.htm`
2. A verification of your Internet domain name which is usually composed of the last two qualifiers of the Web server's name, for instance "`ibm.com`". A so-called "WHOIS" lookup shows who this domain is registered to. The lookup needs to

be done at the *Network Information Center* (NIC) responsible for your domain. The following Webpage (See Figure 11 on page 23 for a sample of this page) contains links to NICs for most Internet domains.
`http://digitalid.verisign.com/server/global/globalStep1.htm`

See Figure 5 on page 15 for sample domain registration information.

You should gather this information before starting the certificate request. Certain pieces of information (such as the name of the organization) must be identical to the information in these documents or your request will be returned.

```
Registrant:
IBM Corporation (IBM-DOM)
   Old Orchard Rd
   Armonk, NY 10504
   US

   Domain Name: IBM.COM

   Administrative Contact, Technical Contact, Zone Contact:
      Trio, Nicholas R  (NRT1)  nrt@WATSON.IBM.COM
      (914) 945-1850
   Billing Contact:
      Trio, Nicholas R  (NRT1)  nrt@WATSON.IBM.COM
      (914) 945-1850

   Record last updated on 09-Jul-98.
   Database last updated on 11-Feb-99 06:27:24 EST.
```

Figure 5. Sample NIC Domain Registration Information for the IBM Domain

2.2.1.1 Creating a Certificate Request File with IKEYMAN

The following steps are necessary to create the certificate request file:

Logon to TSO and enter OMVS (or open a telnet session) on the OS/390 system where your US version of Domino Go Web Server 5.0 for OS/390 is installed. You should do this from a PC that has a Web browser with access to the Internet installed (you will need to do cut-and-paste from your OMVS session into your Web browser). Your user ID must either be a superuser (UID 0) or be authorized to Profile BPX.SUPERUSER in the FACILITY class.

Run the script to enable IKEYMAN (see *Enterprise Web Serving with the Lotus Domino Go WebServer for OS/390*, SG24-2074) and invoke IKEYMAN.

Enter option `3` to create a private/public key pair and a certificate request:

```
 Key database menu

Current key database is /u/graaff/global.kdb

     1  - List/Manage keys and certificates
     2  - List/Manage request keys
     3  - Create new key pair and certificate request
     4  - Receive a certificate issued for your request
     5  - Create a self-signed certificate
     6  - Store a CA certificate
     7  - Show the default key
     8  - Import keys
     9  - Export keys
    10  - List all trusted CAs
    11  - Store encrypted database password

     0  - Exit program

Enter option number (or press ENTER to return to the parent menu):
 ===> 3
```

Enter a file name for the certificate request file; then proceed with each piece of information as prompted:

```
Enter a label for this key.............>
```

You can enter an arbitrary string here.

```
Select desired key size from the following options (512):
    1:    512
    2:    1024
Enter the number corresponding to the key size you want:
```

Select a key size of 1024 bits for the Global Server Certificate's keys.

```
Enter certificate subject name fields in the following.
    Common Name (required).............>
```

The common name must be the address of your Web server, for instance: `wtsc57.itso.ibm.com`. The address must be within your Internet domain. All Web pages accessed through SSL sessions must have an URL that starts with this address or your users will experience problems with their Web browsers.

```
Organization (required).............>
```

The organization name must be identical to the registrant listed in your Internet domain registration and it should also match the company name listed for your D-U-N-S number. If this is not the case, Verisign Inc. will not process your certificate request.

```
Organization Unit (optional).........>
```

This information is not relevant for the verification of the certificate request. You can use it to identify your Web server, for instance: “Home Banking Server” or “ITSO Poughkeepsie”.

```
City/Locality (optional).............>
State/Province (optional).............>
Country Name (required 2 characters)..>
```

Enter the information for the last three fields as appropriate. You can find the correct 2-letter country code (according to ISO 3166) for your country at URL in Appendix B, “List of ISO 3166 Country Codes” on page 43 or at:
`ftp://ftp.ripe.net/iso3166-countrycodes`

IKEYMAN will then create the private/public key pair and the certificate request and will store them in its key database.

To display the list of certificate requests, enter option `2` in the IKEYMAN key database menu:

```
Key database menu

Current key database is /u/graaff/global.kdb

     1  - List/Manage keys and certificates
     2  - List/Manage request keys
     3  - Create new key pair and certificate request
     4  - Receive a certificate issued for your request
     5  - Create a self-signed certificate
     6  - Store a CA certificate
     7  - Show the default key
     8  - Import keys
     9  - Export keys
    10  - List all trusted CAs
    11  - Store encrypted database password

     0  - Exit program

Enter option number (or press ENTER to return to the parent menu):
 ===> 2
```

Then select the key request you created (in this example: “globalibm”). You need to enter option `2` to store the certificate request in an HFS file:

```
 Request Key Menu

Currently selected key: globalibm

Choose one of the following options to proceed.

    1  - Show key information
    2  - Copy the certificate request of this key to a file
    3  - Delete the key

    0  - Exit program

Enter option number (or press ENTER to return to the parent menu):
 ===> 2
```

Enter a name for the certificate request file and exit IKEYMAN after the file has been created. The certificate request file, a file in PEM format (see “PEM Certificate Format” on page 15), cannot be sent to VeriSign Inc. directly. Instead, it has to be pasted into a certificate request created with a Web browser. To prepare this request, open the request file with an editor or browser:

```
BOCHE @ SC57:/u/graaff>
 ===> obrowse globalibmcorp.arm
```

When the certificate request file is displayed, you need to copy its contents to the clipboard. Mark everything between the “Top of Data” and “Bottom of Data” lines including the “BEGIN NEW CERTIFICATE REQUEST”and “END NEW CERTIFICATE REQUEST” lines, but be careful not to extend your mark beyond the last character on the right (column 64) into the blank space. Copy the marked area to the clipboard.

```
 BROWSE -- /u/graaff/globalibmcorp.arm -------------- Line 00000000 Col 001 064
 Command ===>                                           Scroll ===> HALF
******************************** Top of Data ********************************
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBxjCCAS8CAQAwgYUxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJOWTEVMBMGA1UE
BxMMUG91Z2hrZWVwc2llMRgwFgYDVQQKEw9JQk0gQ29ycG9yYXRpb24xGjAYBgNV
BAsTEUlUU08gUG91Z2hrZWVwc2llMRwwGgYDVQQDExN3dHNjNTcuaXRzby5pYm0u
Y29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDSA4YNcHI0ner4kDeBXkEL
AYO2pvJJlnk6sTEF+iVcnJdqrVW3gJlz+YZGc76uAiqeHxaQFO6SvRERJmMG2pZ6
s8N9of0fSCu6KGdRv4JAPjQtqud2JQLyS7on/Axa79pwgXbE8AhL85aQAxPMECoN
LgJHc7LV4KnDGbmb6ys6EQIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYEAqQN9qQ6S
WL3q18znKJ0VcFnpy2gkD2GgZxyLc3lZiSDRTUCD3AVj5azRvaeB4dMxkAHRWXZQ
ERvt+D8AKrQ5qdMolU42KVDFpMknD0/M4uY2ZXDwo84OEJDzSOgngPYNpunHNpmR
WG8Sf41ADIldZFGN2RvTCNOeKDmxDhZD2rI=
-----END NEW CERTIFICATE REQUEST-----
****************************** Bottom of Data ******************************
```

Figure 6. Display of Data in Certificate Request File

2.2.1.2 Creating the Certificate Request With a Web Browser

The request for a Global Server Certificate from VeriSign Inc. must be created with a Web browser. In this example, Netscape Communicator is used; however, it is also possible to use Microsoft Internet Explorer for this task.

Enter the following URL for the Verisign Inc. homepage:
`http://www.verisign.com`.
The page shown in Figure 7 will appear:

Figure 7. The VeriSign Inc. Homepage

The purpose is to request a certificate for a server, so click the button named **Web Site Security**. You will then see the page shown in Figure 8 on page 20

Figure 8. Verisign WebServer Selection Page

At the bottom of this screen you can select the option **Secure Your Web Site Now**. When you click that link, the following screen will be presented, as shown in Figure 9 on page 21.

Figure 9. Verisign Webserver Certificate Request Page

You need to click the link **Global Site Plus** or **Global Site** to request a Global Server Certificate for our Webserver. The next sequence is related to selecting the **Global Site** link.

Figure 10 on page 22, is the first in a series of Web pages that you must navigate through to enroll for the Global Server Certificate. By selecting the **Buy Now** link, the enrollment process will start.

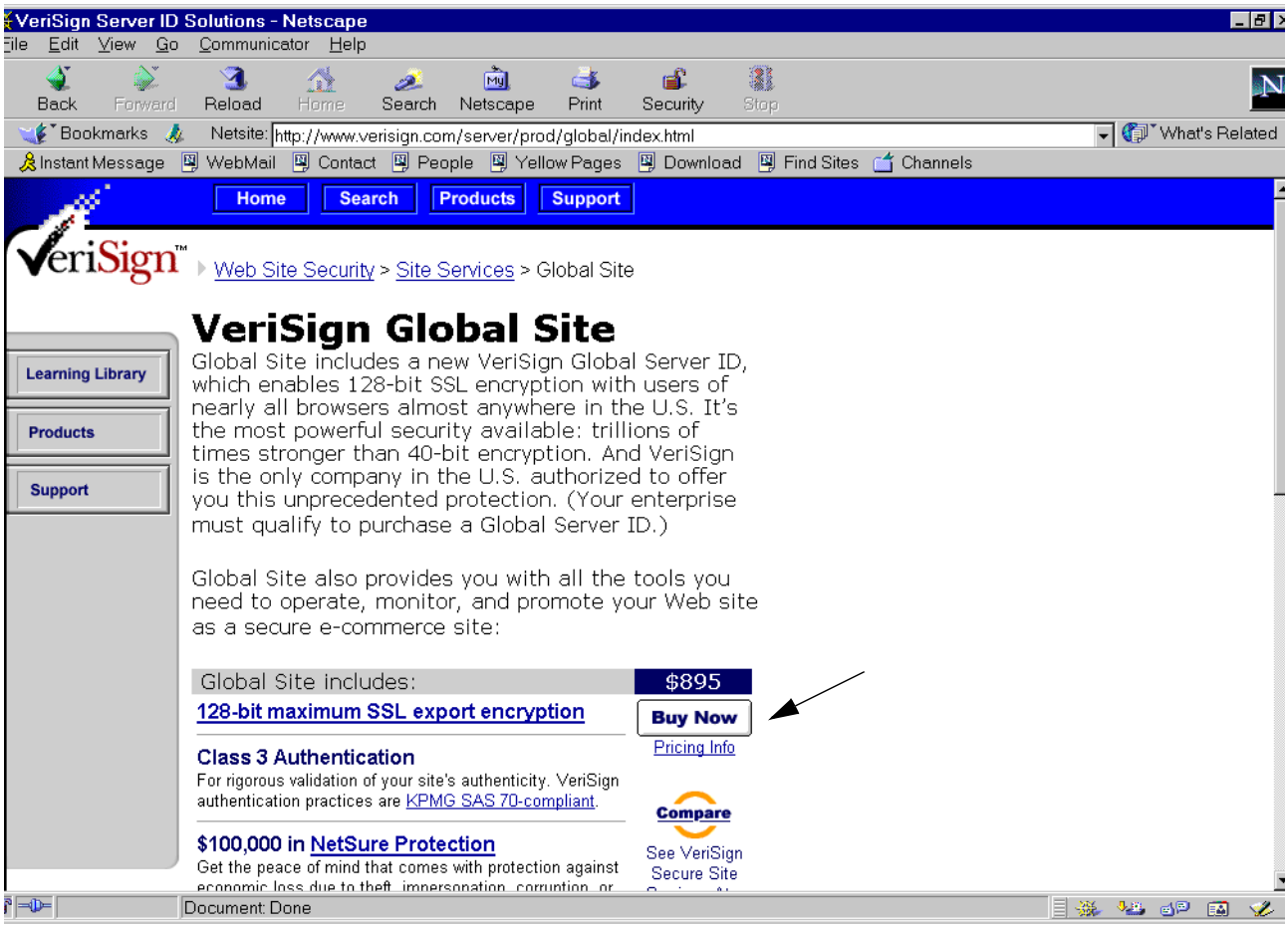


Figure 10. Verisign Global Server Certificate Home Page

A sequence of pages will appear and you need to click **Continue** on each page to get to the next page.

The first page in the series, which we will not show, is a review page that will make sure that you have:

- Reviewed eligibility requirements
- Reviewed the legal agreement
- Determined a payment method
- Have installed your Webserver software
- Reviewed your firewall proxy settings

The page shown in Figure 11 on page 23 is of special interest because it contains links to a number of Network Information Centers (NIC) which are useful to verify the registration of your domain name.

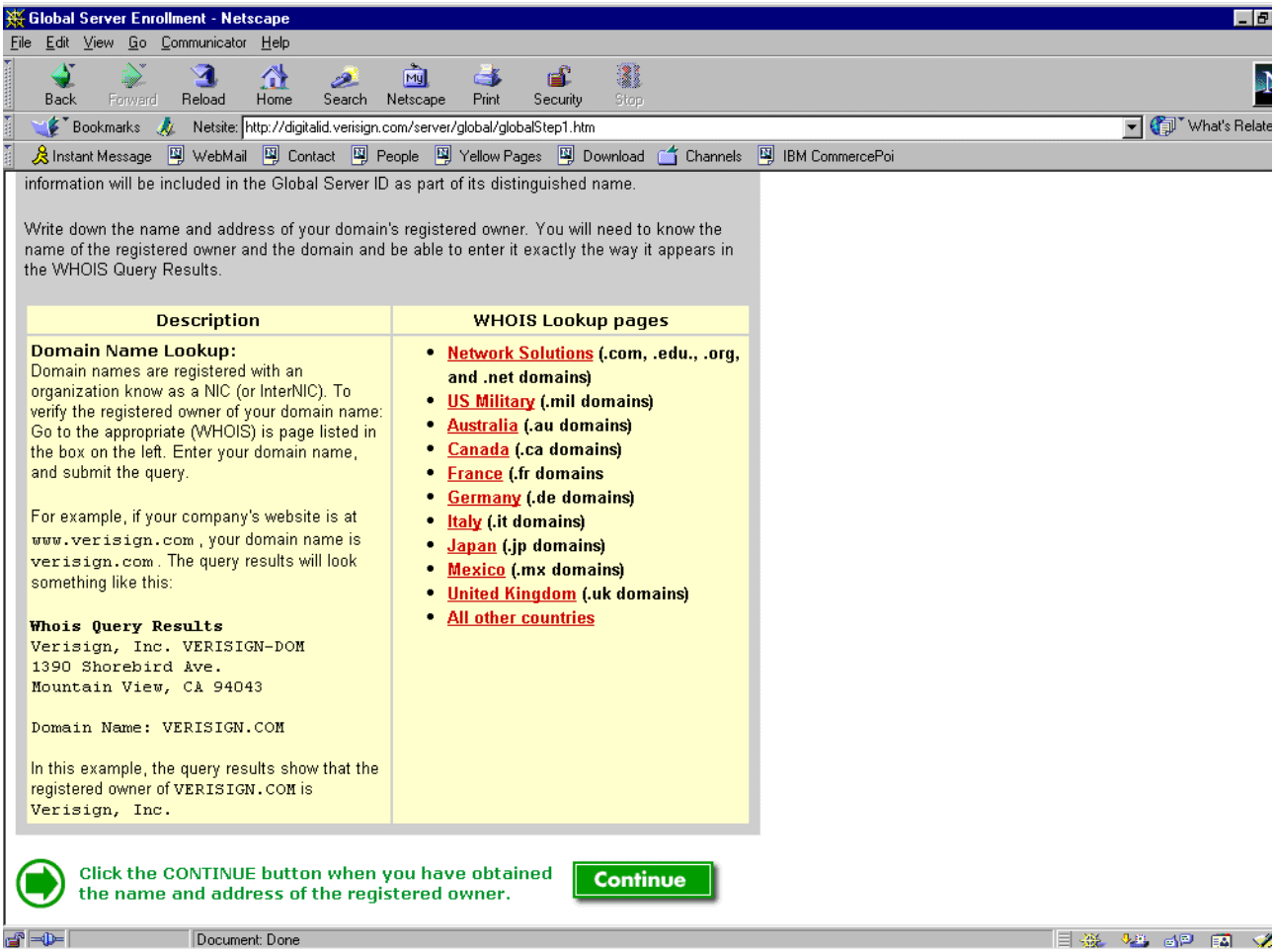


Figure 11. VeriSign Inc. Server Enrollment Domain Lookup Page

As suggested in 2.2.1, “Requesting a Global Server Certificate” on page 14, you should have verified your domain registration before creating the certificate request in order to make sure that the corporation name in your domain registration matches the corporation name in your certificate request. Should that not be the case, there is no point in proceeding any further before you have corrected this mismatch.

The page shown in Figure 12 on page 24 is the most important one. This is the page where you need to enter the data from the certificate request.

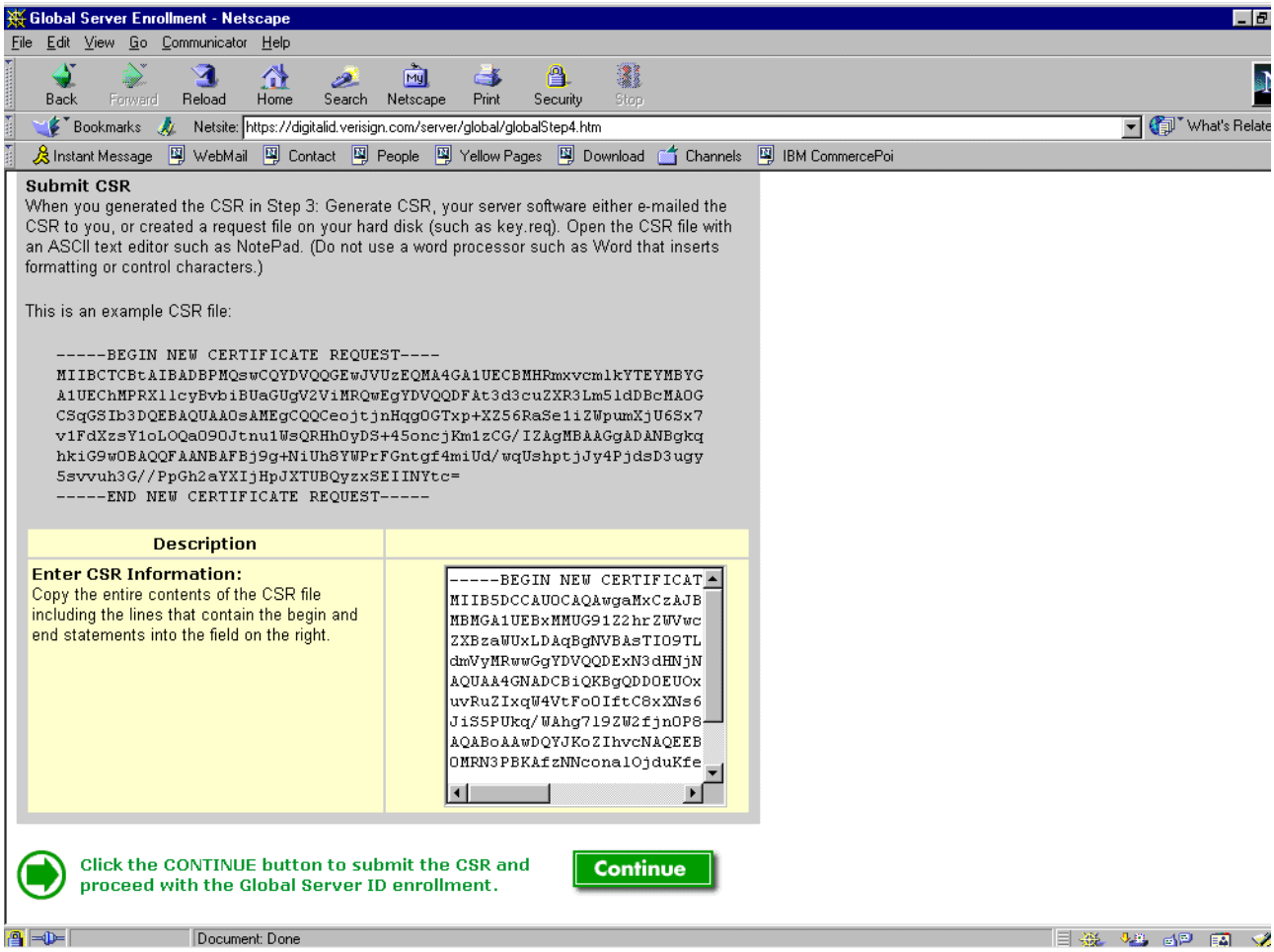


Figure 12. VeriSign Inc. Server Enrollment Certificate Request (CSR) Page

If you followed our step-by-step script, the certificate request data (see Figure 6 on page 18) should still be in your clipboard. Place the cursor into the upper left corner of the text entry field just above the Continue button and paste the data into the field. Your Web page should now look like the sample shown in Figure 12. Click on **Continue** to transmit the data to VeriSign Inc.

If you receive an error with error number FFFFFFFE, the most likely cause is that you included some blank space into the area of the certificate when you copied it to the clipboard. Try again, making sure your mark does not extend beyond column 64.

In all these Web pages, there have been no text-entry fields for information such as the name of your company, the location, and so on. The reason for this is that VeriSign Inc. takes all that information out of the certificate request data (or *Certificate Signing Request* (CSR), as it is called on the VeriSign Inc. Web pages).

The next page, as shown in Figure 13 on page 25, allows you to verify the information gathered from the CSR.

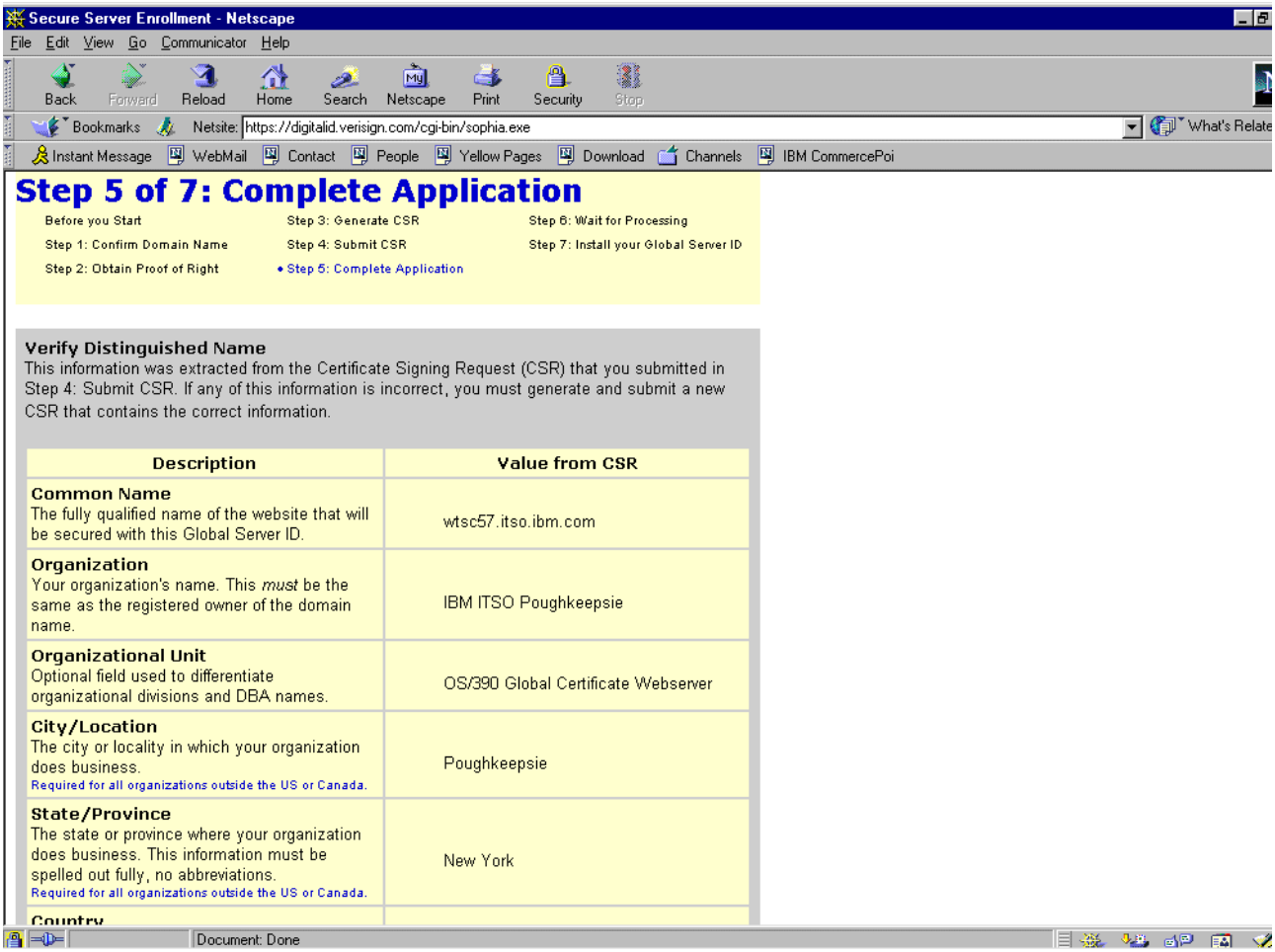


Figure 13. VeriSign Inc. Server Enrollment Completion Page

The information shown on this page should be identical to the information you entered in 2.2.1.1, “Creating a Certificate Request File with IKEYMAN” on page 15.

If you scroll further down (not shown here), you will find a list box where you will need to select the server software vendor. Select **Lotus**. You will also need to specify the person(s) designated as technical contact, organizational contact and billing contact in the forms provided.

Of the three payment options provided (Credit card, Purchase order, Check), we strongly suggest to use, if at all possible, a credit card. Checks will only be accepted when drawn on a US bank and mailing a check from outside the United States will take time.

Enter your D-U-N-S number in the field below the payment information and click the **Accept** button to submit your certificate request to VeriSign Inc.

2.2.2 Storing a Global Server Certificate in Domino Go Web server

When processing is complete, the person designated as technical contact will receive an e-mail message containing the Global Server Certificate and the

certificate of the intermediate Certification Authority (CA). Both certificates need to be stored in the key database of Domino Go Webserver for OS/390.

Do not be concerned about the apparent lack of security in sending an unencrypted e-mail message with your signed certificate over the Internet. Without the private key (which is stored safely in the key database of your Domino Go Webserver), the certificate cannot be misused in any way.

See Figure 14 for the hierarchy of Certification Authority (CA) certificates used with a Global Server Certificate. The self-signed certificate of the Root CA (VeriSign Class 3 Public Primary Certification Authority) is already contained in the key rings of Domino Go Webserver for OS/390 and the Netscape and Microsoft Web browsers. The certificate of the intermediate CA (VeriSign Intermediate CA Global Certificates) is not contained in most key rings. Therefore, it needs to be installed in the key database of Domino Go Webserver for OS/390. The Web server will send it to the client together with the Global Server Certificate during an SSL handshake.

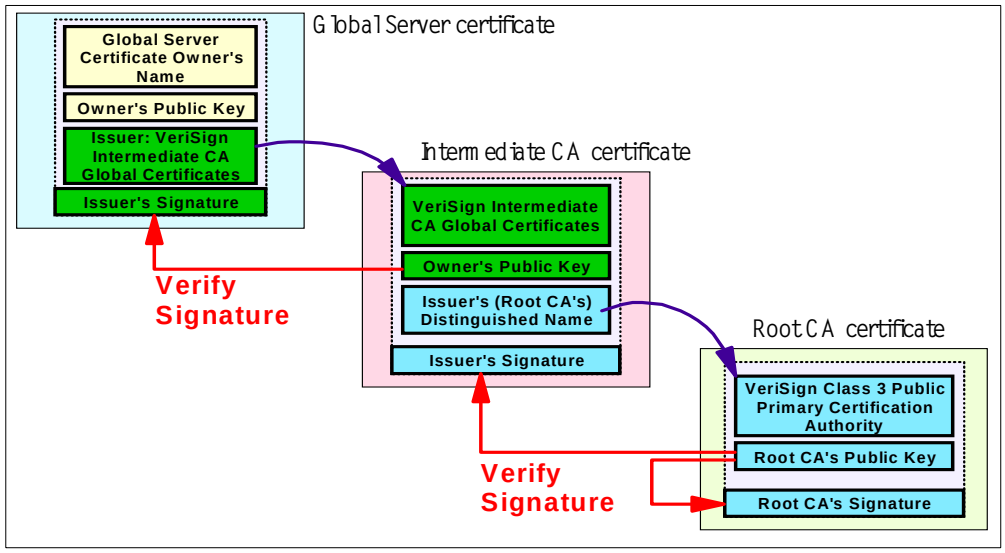


Figure 14. Global Server Certificate Hierarchy

2.2.2.1 Importing the Intermediate CA Certificate

To import the “Intermediate CA Global Certificates” certificate, open the e-mail message from VeriSign Inc. with a suitable mail program (we used Lotus Notes). See Figure 15 for an example of the notification that VeriSign sends out to you.

```
YOUR ORDER NUMBER: 36703281

Dear VeriSign Customer,

CONGRATULATIONS! -- Your VeriSign Global Server ID (certificate),
WTSC57.ITSO.IBM.COM, is included at the end of this message.

VeriSign has digitally signed your Certificate, providing assurance that
your certificate has not been damaged or changed without detection.

Your Digital ID is valid for one year. You may choose to renew it annually.
VeriSign will make a reasonable effort to notify you, via e-Mail, prior to
the expiration of your certificate.

Your new Digital ID qualifies you to participate in VeriSign's Authentic
Site Program at no additional cost. You can promote your site and highlight
your commitment to customer security by displaying the Authentic Site Seal
and including your site in our index of Authentic Sites. Visit
http://www.verisign.com/authentic/intro.html to enroll in this exciting
program.

INSTALLATION:

There are 17 steps involved in installing your ID successfully. Please
print out these instructions and follow them carefully. Then, you
can start enjoying the benefits of 128 bit secure, authenticated communication
with your customers.

PLEASE NOTE: There are TWO certificates attached to this message:

1)The Intermediate CA Certificate, and
2)The Server Subscriber Certificate for your company
```

Figure 15. Example of Verisign’s E-mail Notification

Both the intermediate CA certificate and the Global Server Certificate are contained in this e-mail message.

Copy the whole block under the heading `INTERMEDIATE CA CERTIFICATE` starting with `-----BEGIN CERTIFICATE-----` up to and including `-----END CERTIFICATE-----` to the clipboard.

```
INTERMEDIATE CA CERTIFICATE  (note - this is also referred to as SERVER
CERT CHAIN)

-----BEGIN CERTIFICATE-----
MIIEMTCCA5qgAwIBAgIQI2yXHivGDQv5dGDe8QjDwzANBgkqhkiG9w0BAQIFADBfMQswCQYD
VQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4xNzA1BgNVBAsTLkNsYXNzIDMgUHVi
bGljIFByaW1hcnkgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNOTcwNDE3MDAwMDAwWhcN
MDQwMTA3MjM1OTU5WjCBujEfMB0GA1UEChMWVmVyaVNpZ24gVHJ1c3QgTmV0d29yazEXMBUG
A1UECxMOVmVyaVNpZ24sIEluYy4xMzAxBgNVBAsTKlZlcmlTaWduIEludGVybmF0aW9uYWwg
U2VydmVyIENBIC0gQ2xhc3MgMzFJMEcGA1UECxNAd3d3LnZlcmlzaWduLmNvbS9DUFMgSW5j
b3JwLmJ5IFJlZi4gTElBQklMSVRZIExURC4oYyk5NyBWZXJpU2lnbjCBnzANBgkqhkiG9w0B
AQEFAAOBjQAwgYkCgYEA2IKA6NYZAn0fhRg5JaJlK+G/1AXTvOY2O6rwTGxbtueqPHNFVbLx
veqXQu2aNAoV1Klc9UAl3dkHwTKydWzEyruj/lYncUOqY/UwPpMo5frxCTvzt0100fdcSVq4
wR3Tsor+cDCVQsv+K1GLWjw6+SJPkLICp1OcTzTnqwSye28CAwEAAaOCAZAwggGMMA8GA1Ud
EwQIMAYBAf8CAQAwCwYDVR0PBAQDAgEGMBEGCWCGSAGG+EIBAQQEAwIBBjAgBgNVHSUEGTAX
BgpghkgBhvhFAQgBBglghkgBhvhCBAEwggE1BgNVHSAEggEsMIIBKDCCASQGC2CGSAGG+EUB
BwEBMIIBEzAoBggrBgEFBQcCARYcaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL0NQUzCB5gYI
KwYBBQUHAgIwgdkwFRYOVmVyaVNpZ24sIEluYy4wAwIBARqBv1ZlcmlTaWduJ3MgQ2VydGlm
aWNhdGlvbiBQcmFjdGljZSBTdGF0ZW1lbnQsIHd3dy52ZXJpc2lnbi5jb20vQ1BTLCBnb3Zl
cm5zIHRoaXMgY2VydGlmaWNhdGUgJiBpcyBpbmNvcnBvcmF0ZWQgYnkgcmVmZXJlbmNlIGhl
cmVpbi4gU09NRSBXQVJSQU5USUVTIERJU0NMQUlNRUQgJiBMSUFCSUxJVFkgTFRELiAoYykx
OTk3IFZlcmlTaWduMA0GCSqGSIb3DQEBAgUAA4GBALiMmMMrSPVyzWgNGrN0Y7uxWLaYRSLs
EY3HTjOLYlohJGyawEK0Rak6+2fwkb4YH9VIGZNrjcs3S4bmfZv9jHiZ/4PC/NlVBp4xZkZ9
G3hg9FXUbFXIaWJwfE22iQYFm8hDjswMKNXRjM1GUOMxlmaSESQeSltLZl5lVR5fN5qu
-----END CERTIFICATE-----
```

In your OMVS or telnet session on OS/390, edit a new file, for instance: `oedit globalca.arm`. Paste the contents of the clipboard into the empty edit window and save the file. Do not try to create a file with the certificate in it on the PC and send it to your OS/390 system using FTP, as this will most likely not work. Enter IKEYMAN again and enter option `6`, “Store a CA Certificate”. Enter the file name and a label for the certificate and press Enter to store the certificate.

2.2.2.2 Importing the Global Server Certificate

The Global Server Certificate is contained in the same e-mail message as the Intermediate CA certificate, so all you need to do is to copy the whole block under the heading `SERVER SUBSCRIBER CERTIFICATE` starting with `-----BEGIN CERTIFICATE-----` up to and including `-----END CERTIFICATE-----` to the clipboard.

```
SERVER SUBSCRIBER CERTIFICATE
-----BEGIN CERTIFICATE-----
MIIFKTCCBJKgAwIBAgIQUTn39yDS5PRO0Pg3maWJTjANBgkqhkiG9w0BAQQFADCB
ujEfMB0GA1UEChMWVmVyaVNpZ24gVHJ1c3QgTmV0d29yazEXMBUGA1UECxMOVmVy
aVNpZ24sIEluYy4xMzAxBgNVBAsTKlZlcmlTaWduIEludGVybmF0aW9uYWwgU2Vy
dmVyIENBIC0gQ2xhc3MgMzFJMEcGA1UECxNAd3d3LnZlcmlzaWduLmNvbS9DUFMg
SW5jb3JwLmJ5IFJlZi4gTElBQklMSVRZIExURC4oYyk5NyBWZXJpU2lnbjAeFw05
OTAyMDkwMDAwMDBaFw0wMDAyMDkyMzU5NTlaMIGLMQswCQYDVQQGEwJVUzERMA8G
A1UECBMITmV3IFlvcmsxFTATBgNVBAcUDFBvdWdoa2VlcHNpZTEYMBYGA1UEChQP
SUJNIENvcnBvcmF0aW9uMRowGAYDVQQLFBFJVFNPIFBvdWdoa2VlcHNpZTEcMBoG
A1UEAxQTd3RzYzU3Lml0c28uaWJtLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEAzleCCP5Ns4YEsqaEOntl0FewWTqmUVRHjy4sSpdI0K2QQfxWMKB4xVgB
6ixdzxW8eHszMeg12IbA/SlLMWubVCel+wNj17jmEjTanZH5bIPUxRPCVGsVjGET
waIIVwA8qXYBVeI6p/v8rzYyzAHoMKHjmruqYLOMw8059z3TQQ8CAwEAAaOCAlsw
ggJXMAkGA1UdEwQCMAAwggIfBgNVHQMEggIWMIICEjCCAg4wggIKBgtghkgBhvhF
AQcBATCCAfkWggGnVGhpcyBjZXJ0aWZpY2F0ZSBpbmNvcnBvcmF0ZXMgYnkgcmVm
ZXJlbmNlLCBhbmQgaXRzIHVzZSBpcyBzdHJpY3RseSBzdWJqZWN0IHRvLCB0aGUg
VmVyaVNpZ24gQ2VydGlmaWNhdGlvbiBQcmFjdGljZSBTdGF0ZW1lbnQgKENQUyks
IGF2YWlsYWJsZSBhdDogaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL0NQUzsgYnkg
RS1tYWlsIGF0IENQUy1yZXF1ZXN0c0B2ZXJpc2lnbi5jb207IG9yIGJ5IG1haWwg
YXQgVmVyaVNpZ24sIEluYy4sIDI1OTMgQ29hc3QgQXZlLiwgTW91bnRhaW4gVmll
dywgQ0EgOTQwNDMgVVNBIFRlbC4gKzEgKDQxNSkgOTYxLTg4MzAgQ29weXJpZ2h0
IChjKSAxOTk2IFZlcmlTaWduLCBJbmMuICBBbGwgUmlnaHRzIFJlc2VydmVkLiBD
RVJUQUlOIFdBUlJBTlRJRVMgRElTQ0xBSU1FRCBhbmQgTElBQklMSVRZIExJTUlU
RUQuoA4GDGCGSAGG+EUBBwEBAaEOBgxghkgBhvhFAQcBAQIwLDAqFihodHRwczov
L3d3dy52ZXJpc2lnbi5pb20vcmVwb3NpdG9yeS9DUFMgMBEGCWCGSAGG+EIBAQQE
AwIGQDAUBgNVHSUEDTALBglghkgBhvhCBAEwDQYJKoZIhvcNAQEEBQADgYEA0xG8
LmxKbVX2dlZ6rO2Kqw/J92v8/cY92Ze3H1tUi6iKUM6N9rvjiJeva+ZikHO+QQfQ
umI2+mhBeYuWS+QYZNBYnnAIhHQEFoCMkwS9Iful3pKDaMNaqfhcttJa/JE8sif9
bwueBzH/GYNuvWqQuUKBGLWLGNRuVG+o65y9wiw=
-----END CERTIFICATE-----
```

In your OMVS or telnet session on OS/390, edit a new file, for instance: `oedit globalcert.arm`. Paste the contents of the clipboard into the empty edit window and save the file. Now invoke IKEYMAN and enter option `4` “Receive a certificate issued for your request”. Enter the file name and set the option to make this certificate your default certificate. After you press Enter, the Global Server Certificate will be received and your Domino Go Webserver will now use this certificate for all SSL sessions.

2.3 Secure Sockets Layer with Global Server Certificates

In 1.2, “Secure Sockets Layer (SSL)” on page 16, we described the handshake that takes place between the client (Web browser) and the Web server when an SSL session is established.

When an SSL session is established between the international version of Netscape Navigator/Communicator V.4 or Microsoft Internet Explorer V.4 and a Web server equipped with a Global Server Certificate, a normal SSL handshake is performed initially. Usually, this will mean that the Web server and Web browser will settle on the cipher suite `SSL_RSA_EXPORT_WITH_RC4_40_MD5` which means they will use 512-bit RSA keys for key exchange, RC4 with 40-bit keys for encryption, and MD5 for message authentication.

During the handshake, the browser receives and verifies the server certificate and realizes that this certificate authorizes stronger encryption. You need to remember that the browser sends the list of crypto suites it supports with the

client hello message, before the server sends its certificate. At this point in time, it has no knowledge about the server's Global Server Certificate.

The first handshake is completed with the change cipher spec and finished messages from both client and server. At this point, the client initiates another SSL handshake. This time, in the client hello message, it includes the strong crypto suites such as SSL_RSA_WITH_RC4_128_MD5 (1024-bit RSA keys for key exchange, RC4 with 128-bit keys for encryption, and MD5 for message authentication) and SSL_RSA_WITH_3DES_EDE_CBC_SHA (1024-bit RSA keys for key exchange, triple DES with 168-bit keys for encryption, and SHA-1 for message authentication). After the second handshake is completed, one of the stronger crypto suites will be used.

This double handshake is also known as the *SSL step-up protocol*. Actually, all application data exchanged in the SSL session are encrypted with the stronger encryption protocol. Compared to the use of a US-strength browser, the only drawback is the higher overhead of doing an SSL handshake twice.

2.3.1 Domino Go Webserver 5.0 for OS/390 Performance Improvements

To offset the negative effects on performance from the dual SSL handshake, the PTFs for two APARs that have recently become available should be applied to DGWS 5.0. These APARs are described in the following sections:

2.3.1.1 APAR PQ19981: SSL Performance Improvements

The following areas have been changed by this APAR:

- Message digest usage improvements
- Improvements to the caching algorithms for keys
- Reductions to storage allocations in general

2.3.1.2 APAR PQ22108: Improved Hardware Crypto Support

This APAR adds support for RSA private key encryption and decryption using the S/390 hardware crypto co-processors. In an SSL handshake, the private key decryption process can take over 70 percent of the CPU cycles necessary to process the handshake. By using the OS/390 crypto co-processors to do the work, the CPU utilization can drop dramatically while the number of handshakes per second improves.

For this support to be active, an S/390 processor must have the hardware crypto co-processors installed and active. The ICSF product must also be active.

Users of IBM HTTP Server 5.1 for OS/390 should look for APAR PQ23829.

Appendix A. Dun & Bradstreet Offices

United States Customer Service Center

AUSTIN

Office Hours: Monday-Friday 7:00am-7:00pm CST
Telephone: 1-800-234-3867
Fax: 512-794-7670

Western European Customer Service Centres

AUSTRIA
Office Hours: Monday-Thursday 8.00am-5.00pm, Friday 8.00am-2.30pm GMT +1 hour
Telephone: 43 (1) 588 61 155
Fax: 43 (1) 58 63 359

BELGIUM
Office Hours: Monday-Friday 8.30am-5.30pm GMT +1 hour
Telephone: 32 (2) 778 7222
Fax: 32 (2) 778 7226

DENMARK
Office Hours: Monday-Thursday 8.30am-4.30pm, Friday 8.00am-3.30pm GMT +1 hour
Telephone: 45 (36) 709000
Fax: 45 (36) 70 91 29

FINLAND
Office Hours: Monday-Friday 8.00am - 5.00pm GMT +2 hours
Telephone: 358 (9) 5272361
Fax: 358 (9) 5022940

FRANCE
Office Hours: Monday-Friday 8.30am-6.30pm GMT +1 hour
Telephone: 33 01 41 35 19 19
Fax: 33 01 41 35 19 99 or 33 01 41 35 17 80

GERMANY
Office Hours: Monday-Thursday 8.00am-5.00pm, Friday 8.00am-3.30pm GMT +1 hour
Telephone (49) 69 6609 0
Fax (49) 69 6609 2349

IRELAND
Office Hours: Monday-Friday 9.00am-5.30pm GMT
Telephone: 353 (1) 676 4239
Fax: 353 (1) 676 7149

ISRAEL
Office Hours: Sunday-Thursday 8.00am-5.00pm GMT +2 hours (Closed Friday & Saturday)
Telephone: 972 (3) 510 3355
Fax: 972 (3) 510 3397

ITALY
Office Hours: Monday-Friday 8.30am-5.30pm GMT +1 hour

© Copyright IBM Corp. 1999

Telephone: 39 (2) 2845 5379
Fax: 39 (2) 2845 5596 or 5597

NETHERLANDS
Office Hours: Monday-Friday 8.00am-5.30pm GMT +1 hour
Telephone: 31 (10) 400 9400
Fax: 31 (10) 400 9617

NORTHERN IRELAND
Office Hours: Monday-Friday 9.00am-5.00pm GMT
Telephone: 44 (247) 270 035
Fax: 44 (247) 270 405

NORWAY
Office Hours: Monday-Friday 8.00am - 4.00pm GMT + 1 hour
Telephone: 47 (2) 289 7300
Fax: 47 (2) 289 7303

PORTUGAL
Office Hours: Monday-Friday 9.00am-1.00pm,
2.00pm-6.00pm GMT +1 hour
Telephone: 351 (1) 3146636
Fax: 351 (1) 352 4695

SPAIN
Office Hours: Monday-Friday 8.00am-6.00pm GMT +1 hour
Telephone: (34) 3 280 5858
Fax: (34) 3 280 3350

SWEDEN
Office Hours: Monday - Friday 8.00am - 4.30pm GMT + 1 hour
Telephone: 46 (8) 705 1070
Fax: 46 (8) 735 4263

SWITZERLAND
Office Hours: Monday-Friday 8.00am-6.00pm GMT +1 hour
Telephone: 41-1-735-6111
Fax: 41-1-735-6568

UNITED KINGDOM
Office Hours: Monday-Friday 8.30am-5.30pm GMT
Telephone: 44 (161) 228 7744
Fax: 44 (161) 455 5193

Eastern European, Middle East and African Regions Customer Service Centres

CZECH REPUBLIC
Office Hours: Monday-Friday 8.30am - 5.00pm GMT +1 hour
Telephone: 42 (2) 249 09236
Fax: 42 (2) 298076 or (42) 2 249 11834

HUNGARY
Office Hours: Monday-Thursday 8.00am - 4.30 p.m. GMT + 1 hour
Friday 8.00am - 3.00 p.m.
Telephone: 36 (1) 267 4190
Fax: 36 (1) 267 4198

POLAND

Office Hours: Monday-Friday 9.00am-5.00pm GMT + 1 hour
Telephone: 48 (2) 6257202 or 6257203
or 6257204
Fax: 48 (2) 6257200

RUSSIA
Office Hours: Monday-Friday 9.30am-6.00pm GMT +3 hours
Telephone: 7 (095) 940 1816
Fax: 7 (095) 940 1708 or 940 1702

SOUTH AFRICA
Office Hours: Monday-Friday 9.00am-5.00pm GMT +2 hours
Telephone: 27 11 488 2334
Fax: 27 11 642 1010

ZIMBABWE
Office Hours: Monday-Friday 9.00am-5.00pm GMT + 2 hours
Telephone: 263 (4) 70 4891 or 72 6169
Fax: 263 (4) 72 6189

Information centre for all other countries in Eastern
Europe, Middle East & Africa
Office Hours: Monday-Friday 9.00am-5.00pm GMT
Telephone: 44 (1494) 423858
Fax: 44 (1494) 422280/422281

Asia Pacific, Canada, Latin America Customer Service Centers

CENTRAL AMERICA, CARIBBEAN ISLANDS,
NORTHERN CONE OF SOUTH AMERICA
Office Hours: Monday - Friday 8:00am - 5:00pm, EST
Telephone: (954) 893-4072
Fax: (954) 893-4080
E-mail: calcanov@dnb.com

ARGENTINA
Office Hours: Monday - Friday 8:30am - 12:00pm,
1:00pm -5:30 pm, GMT -3 hours
Telephone: (54) (1) 318-3124
Fax: (54) (1) 318-3199

AUSTRALIA
Office Hours: Monday - Friday: 8:00am - 5:30pm, GMT +11 hours
Telephone: (61) (3) 982 83448
Fax: (61) (3) 982 83447 or (61) (3) 982 83300

BRAZIL
Office Hours: Monday - Friday 8:00am - 11:30am;
12:30pm - 5:00pm, GMT -3 hours
Telephone: 5511-888-6817
Fax: 5511-888-6809
E-mail: cliente@dnb.com

CANADA
Office Hours: Monday - Friday: 8:00am - 7:00pm EST, GMT -5 hours
Telephone: 1-800-463-6362, or (416) 463-6362
Fax: (905) 568-5815

CHINA
Office Hours: Monday - Friday: 8:30am - 5:30pm, GMT +8 hours
Telephone: (8621) 6218-9402
Fax: (8621) 6218-8103

HONG KONG
Office Hours: Monday - Friday: 9:00am - 5:30pm, GMT +8 hours
Telephone: (852) 2561-6333
Fax: (852) 2811-0053

INDIA
Office Hours: Monday - Friday: 9:00am - 6:00pm, GMT +5½ hours
Telephone: (91)(22)857-4190/92/94
Fax: (91) (22)857-2060
E-mail: dbindia@bom2.vsnl.net.in

JAPAN
Office Hours: Monday - Friday: 9:00am - 5:30pm, GMT +9 hours
Telephone: (81) (3) 3481-3561
Fax: (81) (3) 3481-3570

KOREA
Office Hours: Monday - Friday: 8:30am - 5:45pm, GMT +8 hours
Telephone: (82) (2) 761-1070
Fax: (82) (2) 761-1075

MALAYSIA
Office Hours: Monday - Friday: 8:30am - 5:45pm, GMT +8 hours
Telephone: (60) 3 262 7995
Fax: (60) 3 264 4877

MEXICO
Office Hours: Monday - Friday: 8:30am - 5:30pm, GMT -6 hours
Telephone: (525) 208-5066
Fax : (525) 511-0065

NEW ZEALAND
Office Hours: Monday - Friday: 8:30am - 5:00pm, GMT +11 hours
Telephone: (64) (9) 377-7700
Fax: (64) (9) 309-2050

PERU
Office Hours: Monday - Friday: 9:00am to 4:45pm, GMT -5 hours
Telephone: (51)(14) 335-533
Fax: (51) (14) 332-897

SINGAPORE
Office Hours: Monday - Friday: 8:30am - 5:45pm, GMT +8 hours
Telephone: (65) 334-3336
Fax: (65) 334-2465

TAIWAN
Office Hours: Monday - Friday: 9:00am - 5:30pm, GMT +8 hours
Telephone: (886) (2) 756-2922
Fax: (886) (2) 749-1936

Appendix B. List of ISO 3166 Country Codes

Some Codes from ISO 3166

Updated by the RIPE Network Coordination Centre.

Source: ISO 3166 Maintenance Agency

Latest change: Thu Aug 7 17:59:51 MET DST 1997

Country	A 2	A 3	Number
AFGHANISTAN	AF	AFG	004
ALBANIA	AL	ALB	008
ALGERIA	DZ	DZA	012
AMERICAN SAMOA	AS	ASM	016
ANDORRA	AD	AND	020
ANGOLA	AO	AGO	024
ANGUILLA	AI	AIA	660
ANTARCTICA	AQ	ATA	010
ANTIGUA AND BARBUDA	AG	ATG	028
ARGENTINA	AR	ARG	032
ARMENIA	AM	ARM	051
ARUBA	AW	ABW	533
AUSTRALIA	AU	AUS	036
AUSTRIA	AT	AUT	040
AZERBAIJAN	AZ	AZE	031
BAHAMAS	BS	BHS	044
BAHRAIN	BH	BHR	048
BANGLADESH	BD	BGD	050
BARBADOS	BB	BRB	052
BELARUS	BY	BLR	112
BELGIUM	BE	BEL	056
BELIZE	BZ	BLZ	084
BENIN	BJ	BEN	204
BERMUDA	BM	BMU	060
BHUTAN	BT	BTN	064
BOLIVIA	BO	BOL	068
BOSNIA AND HERZEGOWINA	BA	BIH	070
BOTSWANA	BW	BWA	072
BOUVET ISLAND	BV	BVT	074
BRAZIL	BR	BRA	076
BRITISH INDIAN OCEAN TERRITORY	IO	IOT	086
BRUNEI DARUSSALAM	BN	BRN	096
BULGARIA	BG	BGR	100
BURKINA FASO	BF	BFA	854
BURUNDI	BI	BDI	108
CAMBODIA	KH	KHM	116
CAMEROON	CM	CMR	120
CANADA	CA	CAN	124
CAPE VERDE	CV	CPV	132
CAYMAN ISLANDS	KY	CYM	136
CENTRAL AFRICAN REPUBLIC	CF	CAF	140
CHAD	TD	TCD	148
CHILE	CL	CHL	152
CHINA	CN	CHN	156
CHRISTMAS ISLAND	CX	CXR	162

© Copyright IBM Corp. 1999

COCOS (KEELING) ISLANDS	CC	CCK	166
COLOMBIA	CO	COL	170
COMOROS	KM	COM	174
CONGO	CG	COG	178
CONGO, THE DEMOCRATIC REPUBLIC OF THE	CD	COD	180
COOK ISLANDS	CK	COK	184
COSTA RICA	CR	CRI	188
COTE D'IVOIRE	CI	CIV	384
CROATIA (local name: Hrvatska)	HR	HRV	191
CUBA	CU	CUB	192
CYPRUS	CY	CYP	196
CZECH REPUBLIC	CZ	CZE	203
DENMARK	DK	DNK	208
DJIBOUTI	DJ	DJI	262
DOMINICA	DM	DMA	212
DOMINICAN REPUBLIC	DO	DOM	214
EAST TIMOR	TP	TMP	626
ECUADOR	EC	ECU	218
EGYPT	EG	EGY	818
EL SALVADOR	SV	SLV	222
EQUATORIAL GUINEA	GQ	GNQ	226
ERITREA	ER	ERI	232
ESTONIA	EE	EST	233
ETHIOPIA	ET	ETH	231
FALKLAND ISLANDS (MALVINAS)	FK	FLK	238
FAROE ISLANDS	FO	FRO	234
FIJI	FJ	FJI	242
FINLAND	FI	FIN	246
FRANCE	FR	FRA	250
FRANCE, METROPOLITAN	FX	FXX	249
FRENCH GUIANA	GF	GUF	254
FRENCH POLYNESIA	PF	PYF	258
FRENCH SOUTHERN TERRITORIES	TF	ATF	260
GABON	GA	GAB	266
GAMBIA	GM	GMB	270
GEORGIA	GE	GEO	268
GERMANY	DE	DEU	276
GHANA	GH	GHA	288
GIBRALTAR	GI	GIB	292
GREECE	GR	GRC	300
GREENLAND	GL	GRL	304
GRENADA	GD	GRD	308
GUADELOUPE	GP	GLP	312
GUAM	GU	GUM	316
GUATEMALA	GT	GTM	320
GUINEA	GN	GIN	324
GUINEA-BISSAU	GW	GNB	624
GUYANA	GY	GUY	328
HAITI	HT	HTI	332
HEARD AND MC DONALD ISLANDS	HM	HMD	334
HOLY SEE (VATICAN CITY STATE)	VA	VAT	336
HONDURAS	HN	HND	340
HONG KONG	HK	HKG	344
HUNGARY	HU	HUN	348
ICELAND	IS	ISL	352
INDIA	IN	IND	356
INDONESIA	ID	IDN	360
IRAN (ISLAMIC REPUBLIC OF)	IR	IRN	364

IRAQ	IQ	IRQ	368
IRELAND	IE	IRL	372
ISRAEL	IL	ISR	376
ITALY	IT	ITA	380
JAMAICA	JM	JAM	388
JAPAN	JP	JPN	392
JORDAN	JO	JOR	400
KAZAKHSTAN	KZ	KAZ	398
KENYA	KE	KEN	404
KIRIBATI	KI	KIR	296
KOREA, DEMOCRATIC PEOPLE'S REPUBLIC OF	KP	PRK	408
KOREA, REPUBLIC OF	KR	KOR	410
KUWAIT	KW	KWT	414
KYRGYZSTAN	KG	KGZ	417
LAO PEOPLE'S DEMOCRATIC REPUBLIC	LA	LAO	418
LATVIA	LV	LVA	428
LEBANON	LB	LBN	422
LESOTHO	LS	LSO	426
LIBERIA	LR	LBR	430
LIBYAN ARAB JAMAHIRIYA	LY	LBY	434
LIECHTENSTEIN	LI	LIE	438
LITHUANIA	LT	LTU	440
LUXEMBOURG	LU	LUX	442
MACAU	MO	MAC	446
MACEDONIA, THE FORMER YUGOSLAV REPUBLIC OF	MK	MKD	807
MADAGASCAR	MG	MDG	450
MALAWI	MW	MWI	454
MALAYSIA	MY	MYS	458
MALDIVES	MV	MDV	462
MALI	ML	MLI	466
MALTA	MT	MLT	470
MARSHALL ISLANDS	MH	MHL	584
MARTINIQUE	MQ	MTQ	474
MAURITANIA	MR	MRT	478
MAURITIUS	MU	MUS	480
MAYOTTE	YT	MYT	175
MEXICO	MX	MEX	484
MICRONESIA, FEDERATED STATES OF	FM	FSM	583
MOLDOVA, REPUBLIC OF	MD	MDA	498
MONACO	MC	MCO	492
MONGOLIA	MN	MNG	496
MONTSERRAT	MS	MSR	500
MOROCCO	MA	MAR	504
MOZAMBIQUE	MZ	MOZ	508
MYANMAR	MM	MMR	104
NAMIBIA	NA	NAM	516
NAURU	NR	NRU	520
NEPAL	NP	NPL	524
NETHERLANDS	NL	NLD	528
NETHERLANDS ANTILLES	AN	ANT	530
NEW CALEDONIA	NC	NCL	540
NEW ZEALAND	NZ	NZL	554
NICARAGUA	NI	NIC	558
NIGER	NE	NER	562
NIGERIA	NG	NGA	566
NIUE	NU	NIU	570
NORFOLK ISLAND	NF	NFK	574
NORTHERN MARIANA ISLANDS	MP	MNP	580

NORWAY	NO	NOR	578
OMAN	OM	OMN	512
PAKISTAN	PK	PAK	586
PALAU	PW	PLW	585
PANAMA	PA	PAN	591
PAPUA NEW GUINEA	PG	PNG	598
PARAGUAY	PY	PRY	600
PERU	PE	PER	604
PHILIPPINES	PH	PHL	608
PITCAIRN	PN	PCN	612
POLAND	PL	POL	616
PORTUGAL	PT	PRT	620
PUERTO RICO	PR	PRI	630
QATAR	QA	QAT	634
REUNION	RE	REU	638
ROMANIA	RO	ROM	642
RUSSIAN FEDERATION	RU	RUS	643
RWANDA	RW	RWA	646
SAINT KITTS AND NEVIS	KN	KNA	659
SAINT LUCIA	LC	LCA	662
SAINT VINCENT AND THE GRENADINES	VC	VCT	670
SAMOA	WS	WSM	882
SAN MARINO	SM	SMR	674
SAO TOME AND PRINCIPE	ST	STP	678
SAUDI ARABIA	SA	SAU	682
SENEGAL	SN	SEN	686
SEYCHELLES	SC	SYC	690
SIERRA LEONE	SL	SLE	694
SINGAPORE	SG	SGP	702
SLOVAKIA (Slovak Republic)	SK	SVK	703
SLOVENIA	SI	SVN	705
SOLOMON ISLANDS	SB	SLB	090
SOMALIA	SO	SOM	706
SOUTH AFRICA	ZA	ZAF	710
SOUTH GEORGIA AND THE SOUTH SANDWICH ISLANDS	GS	SGS	239
SPAIN	ES	ESP	724
SRI LANKA	LK	LKA	144
ST. HELENA	SH	SHN	654
ST. PIERRE AND MIQUELON	PM	SPM	666
SUDAN	SD	SDN	736
SURINAME	SR	SUR	740
SVALBARD AND JAN MAYEN ISLANDS	SJ	SJM	744
SWAZILAND	SZ	SWZ	748
SWEDEN	SE	SWE	752
SWITZERLAND	CH	CHE	756
SYRIAN ARAB REPUBLIC	SY	SYR	760
TAIWAN, PROVINCE OF CHINA	TW	TWN	158
TAJIKISTAN	TJ	TJK	762
TANZANIA, UNITED REPUBLIC OF	TZ	TZA	834
THAILAND	TH	THA	764
TOGO	TG	TGO	768
TOKELAU	TK	TKL	772
TONGA	TO	TON	776
TRINIDAD AND TOBAGO	TT	TTO	780
TUNISIA	TN	TUN	788
TURKEY	TR	TUR	792
TURKMENISTAN	TM	TKM	795
TURKS AND CAICOS ISLANDS	TC	TCA	796

TUVALU	TV	TUV	798
UGANDA	UG	UGA	800
UKRAINE	UA	UKR	804
UNITED ARAB EMIRATES	AE	ARE	784
UNITED KINGDOM	GB	GBR	826
UNITED STATES	US	USA	840
UNITED STATES MINOR OUTLYING ISLANDS	UM	UMI	581
URUGUAY	UY	URY	858
UZBEKISTAN	UZ	UZB	860
VANUATU	VU	VUT	548
VENEZUELA	VE	VEN	862
VIET NAM	VN	VNM	704
VIRGIN ISLANDS (BRITISH)	VG	VGB	092
VIRGIN ISLANDS (U.S.)	VI	VIR	850
WALLIS AND FUTUNA ISLANDS	WF	WLF	876
WESTERN SAHARA	EH	ESH	732
YEMEN	YE	YEM	887
YUGOSLAVIA	YU	YUG	891
ZAMBIA	ZM	ZMB	894
ZIMBABWE	ZW	ZWE	716

Appendix C. Special Notices

This publication is intended to help technical support staff and webmasters install, configure, and use Global Server Certificates for use with the Lotus Domino Go Webserver for OS/390. The information in this publication is not intended as the specification of any programming interfaces that are provided by Lotus Domino Go Webserver for OS/390. See the PUBLICATIONS section of the IBM Programming Announcement for Lotus Domino Go Webserver for OS/390 for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, NY 10594 USA.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM ("vendor") products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

Any performance data contained in this document was determined in a controlled environment, and therefore, the results that may be obtained in other operating

© Copyright IBM Corp. 1999

environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

IBM ®	DB2
MQ	IMS
OS/390	Parallel Sysplex
RS/6000	RACF
SP	S/390
System/390	3090

The following terms are trademarks of other companies:

C-bus is a trademark of Corollary, Inc. in the United States and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries.

PC Direct is a trademark of Ziff Communications Company in the United States and/or other countries and is used by IBM Corporation under license.

ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States and/or other countries. (For a complete list of Intel trademarks see www.intel.com/dradmarx.htm)

UNIX is a registered trademark in the United States and/or other countries licensed exclusively through X/Open Company Limited.

Other company, product, and service names may be trademarks or service marks of others.

Appendix D. Related Publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

D.1 International Technical Support Organization Publications

For information on ordering these ITSO publications see “How to Get ITSO Redbooks” on page 45.

- *Enterprise Web Serving with the Lotus Domino Go Webserver for OS/390*, SG24-2074

D.2 Redbooks on CD-ROMs

Redbooks are also available on the following CD-ROMs**:**

CD-ROM Title	Collection Kit Number
System/390 Redbooks Collection	SK2T-2177
Networking and Systems Management Redbooks Collection	SK2T-6022
Transaction Processing and Data Management Redbook	SK2T-8038
Lotus Redbooks Collection	SK2T-8039
Tivoli Redbooks Collection	SK2T-8044
AS/400 Redbooks Collection	SK2T-2849
RS/6000 Redbooks Collection (HTML, BkMgr)	SK2T-8040
RS/6000 Redbooks Collection (PostScript)	SK2T-8041
RS/6000 Redbooks Collection (PDF Format)	SK2T-8043
Application Development Redbooks Collection	SK2T-8037

D.3 Other Publications

These publications are also relevant as further information sources:

- *Domino Go Webserver Webmaster’s Guide Rel.5 for OS/390*, SC31-8691

© Copyright IBM Corp. 1999

How to Get ITSO Redbooks

This section explains how both customers and IBM employees can find out about ITSO redbooks, redpieces, and CD-ROMs. A form for ordering books and CD-ROMs by fax or e-mail is also provided.

- **Redbooks Web Site** `http://www.redbooks.ibm.com/`

  Search for, view, download or order hardcopy/CD-ROM redbooks from the redbooks web site. Also read redpieces and download additional materials (code samples or diskette/CD-ROM images) from this redbooks site.

  Redpieces are redbooks in progress; not all redbooks become redpieces and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

- **E-mail Orders**

  Send orders via e-mail including information from the redbooks fax order form to:

	e-mail address
In United States	usib6fpl@ibmmail.com
Outside North America	Contact information is in the “How to Order” section at this site: `http://www.elink.ibmlink.ibm.com/pbl/pbl/`

- **Telephone Orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	Country coordinator phone number is in the “How to Order” section at this site: `http://www.elink.ibmlink.ibm.com/pbl/pbl/`

- **Fax Orders**

United States (toll free)	1-800-445-9269
Canada	1-403-267-4455
Outside North America	Fax phone number is in the “How to Order” section at this site: `http://www.elink.ibmlink.ibm.com/pbl/pbl/`

This information was current at the time of publication, but is continually subject to change. The latest information for customer may be found at `http://www.redbooks.ibm.com/` and for IBM employees at `http://w3.itso.ibm.com/`.

IBM Intranet for Employees

IBM employees may register for information on workshops, residencies, and redbooks by accessing the IBM Intranet Web site at `http://w3.itso.ibm.com/` and clicking the ITSO Mailing List button. Look in the Materials repository for workshops, presentations, papers, and Web pages developed and written by the ITSO technical professionals; click the Additional Materials button. Employees may also view redbook. residency, and workshop announcements at `http://inews.ibm.com/`.

© Copyright IBM Corp. 1999

IBM Redbook Fax Order Form

Please send me the following:

Title	Order Number	Quantity

First name	Last name	
Company		
Address		
City	Postal code	Country
Telephone number	Telefax number	VAT number

☐ Invoice to customer number _____

☐ Credit card number _____

Credit card expiration date	Card issued to	Signature

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

Index

© Copyright IBM Corp. 1999

ITSO Redbook Evaluation

Global Server Certificate Usage with OS/390 Webservers
SG24-5623-00

Your feedback is very important to help us maintain the quality of ITSO redbooks. **Please complete this questionnaire and return it using one of the following methods:**

- Use the online evaluation form found at http://www.redbooks.ibm.com
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to redbook@us.ibm.com

Which of the following best describes you?
_ **Customer** _ **Business Partner** _ **Solution Developer** _ **IBM employee**
_ **None of the above**

Please rate your overall satisfaction with this book using the scale:
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction _____

Please answer the following questions:

Was this redbook published in time for your needs? Yes___ No___

If no, please explain:

_____

_____

_____

_____

What other redbooks would you like to see published?

_____

_____

_____

Comments/Suggestions: (THANK YOU FOR YOUR FEEDBACK!)

_____

_____

_____

_____

_____

© Copyright IBM Corp. 1999

SG24-5623-00

Printed in the U.S.A.

Global Server Certificate Usage with OS/390 Webservers

SG24-5623-00