

Name Store Connection Management Recommendations for Registrars

1.0

Thursday, September 23, 2004



VeriSign Global Registry Services Proprietary Information

This document is the property of VeriSign Global Registry Services, Inc. It may be used by recipient only for the purpose for which it was transmitted and will be returned upon request or when no longer needed by recipient. It may not be copied or communicated without the prior written consent of VeriSign Global Registry Services.

COPYRIGHT NOTIFICATION

Copyright © 2004, VeriSign, Inc. All rights reserved.

VERISIGN GLOBAL REGISTRY SERVICES PROPRIETARY INFORMATION

This document is the property of VeriSign, Inc. Information contained herein may include trade secrets and confidential information belonging to VeriSign. Unauthorized disclosure without the express written consent of VeriSign, Inc. is prohibited. It may be used by recipient only for the purpose for which it was transmitted and will be returned upon request or when no longer needed by recipient. It may not be copied or communicated without the prior written consent of VeriSign, Inc..

DISCLAIMER AND LIMITATION OF LIABILITY

VeriSign, Inc. has made efforts to ensure the accuracy and completeness of the information in this document. However, VeriSign, Inc. makes no warranties of any kind (whether express, implied or statutory) with respect to the information contained herein. VeriSign, Inc. assumes no liability to any party for any loss or damage (whether direct or indirect) caused by any errors, omissions or statements of any kind contained in this document. Further, VeriSign, Inc. assumes no liability arising from the application or use of the product or service described herein and specifically disclaims any representation that the products or services described do not infringe upon any existing or future intellectual property rights. Nothing herein grants the reader any license to make, use, or sell equipment or products constructed in accordance with this document. Finally, all rights and privileges related to any intellectual property right described in this document are vested in the patent, trademark, or service mark owner, and no other person may exercise such rights without express permission, authority, or license secured from the patent, trademark, or service mark owner.

VeriSign Inc. reserves the right to make changes to any information herein without further notice.

NOTICE AND CAUTION

Concerning U.S. Patent or Trademark Rights

The inclusion in this document, the associated on-line file, or the associated software of any information covered by any patent, trademark, or service mark rights will not constitute nor imply a grant of, or authority to exercise, any right or privilege protected by such patent, trademark, or service mark. All such rights and privileges are vested in the patent, trademark, or service mark owner, and no other person may exercise such rights without express permission, authority, or license secured from the patent, trademark, or service mark owner.

This publication was created using Microsoft® Word 2000 for Windows™ by Microsoft Corporation.

Microsoft is a registered trademark and Windows is a trademark of Microsoft Corporation.



VeriSign® Global Registry Services

21345 Ridgetop Circle

Dulles, VA 20166-6503

E-mail: info@verisign-grs.com

Internet: <http://www.verisign-grs.com>

Contents

1.	Executive Summary	4
2.	Protocols and Transports.....	4
2.1	What is a “protocol”?	4
2.2	What does “protocol” mean in Name Store?	4
2.3	What is a “transport”?	5
2.4	What does “transport” mean in Name Store?.....	5
3.	Name Store Access by Registrars	6
4.	Best Practices for Accessing RRP/SSL	8
5.	Best Practices for Accessing EPP/SSL.....	9
6.	Best Practices for Accessing EPP/HTTPS.....	10
7.	Managing Connections for Requests Related to RccTLD	11
8.	SSL Certificates	11
9.	Conclusion	13

1. Executive Summary

The Name Store Consolidated Project offers a unified registry service that provides an online transaction system and a registrar tool for the various top level domain names (TLDs) that the VeriSign Naming and Directory Service is in the business of managing.

This document describes how registrars can effectively connect to the Name Store system in order to achieve the best possible results for order processing.

2. Protocols and Transports

2.1 *What is a “protocol”?*

A protocol is a formal description of message formats and the rules the two communicating systems must follow to exchange those messages need to be defined. A protocol can also describe low-level details of machine-to-machine interfaces (e.g., the order in which bits and bytes are sent across wire) or high-level exchanges between application programs (e.g., the way in which two programs transfer a file across the Internet).

2.2 *What does “protocol” mean in Name Store?*

In Name Store, we define a protocol to be a formal description of the provisioning application data that the communications systems (registrars and registry) will use to communicate with each other.

To enable registrars to sell domain names, Name Store supports two different protocols which are incorporated in the Name Store Consolidated project. They are RRP and EPP:

1. RRP (Registry Registrar Protocol)

RRP is a connection oriented application layer protocol for provisioning objects (domain, hosts and other related objects) shared in a common repository. This is a plain text based protocol that supports a flat data structure.

2. EPP (Extensible Provisioning Protocol)

EPP is an IETF standard connection oriented application layer protocol for provisioning objects (domain, hosts and other related objects) shared in a common repository. This is an XML based protocol that supports a hierarchical and extensible data structure.

2.3 What is a “transport”?

A transport provides an end-to-end control of a communication session between applications to exchange data reliably in the network. TCP/IP is the most popular transport layer responsible for maintaining reliable end-to-end communications in the Internet. But, TCP/IP by itself does not provide a secure communication channel. Hence, SSL (Secure Socket Layer) is commonly used to provide a secure communication channel between the communicating parties.

HTTP can also be used as a higher level transport, built over TCP/IP. When HTTP is used over a secure TCP/IP channel, it is called HTTPS.

2.4 What does “transport” mean in Name Store?

Name Store supports two transports for registrars to communicate with the Name Store application for order processing. They are SSL and HTTPS:

1. TCP/SSL (Secure TCP)

Allows registrars to open an SSL connection with the Name Store system and send EPP or RRP commands for order processing.

2. HTTPS (Secure HTTP)

Allows registrars to open an HTTPS connection with the Name Store system and send EPP commands for order processing.

Note: Technically speaking, both the transports named above (TCP/SSL and HTTPS) use TCP/IP as the underlying data communications layer. We have

named them TCP/SSL and HTTPS to easily distinguish between the two for ease of reference.

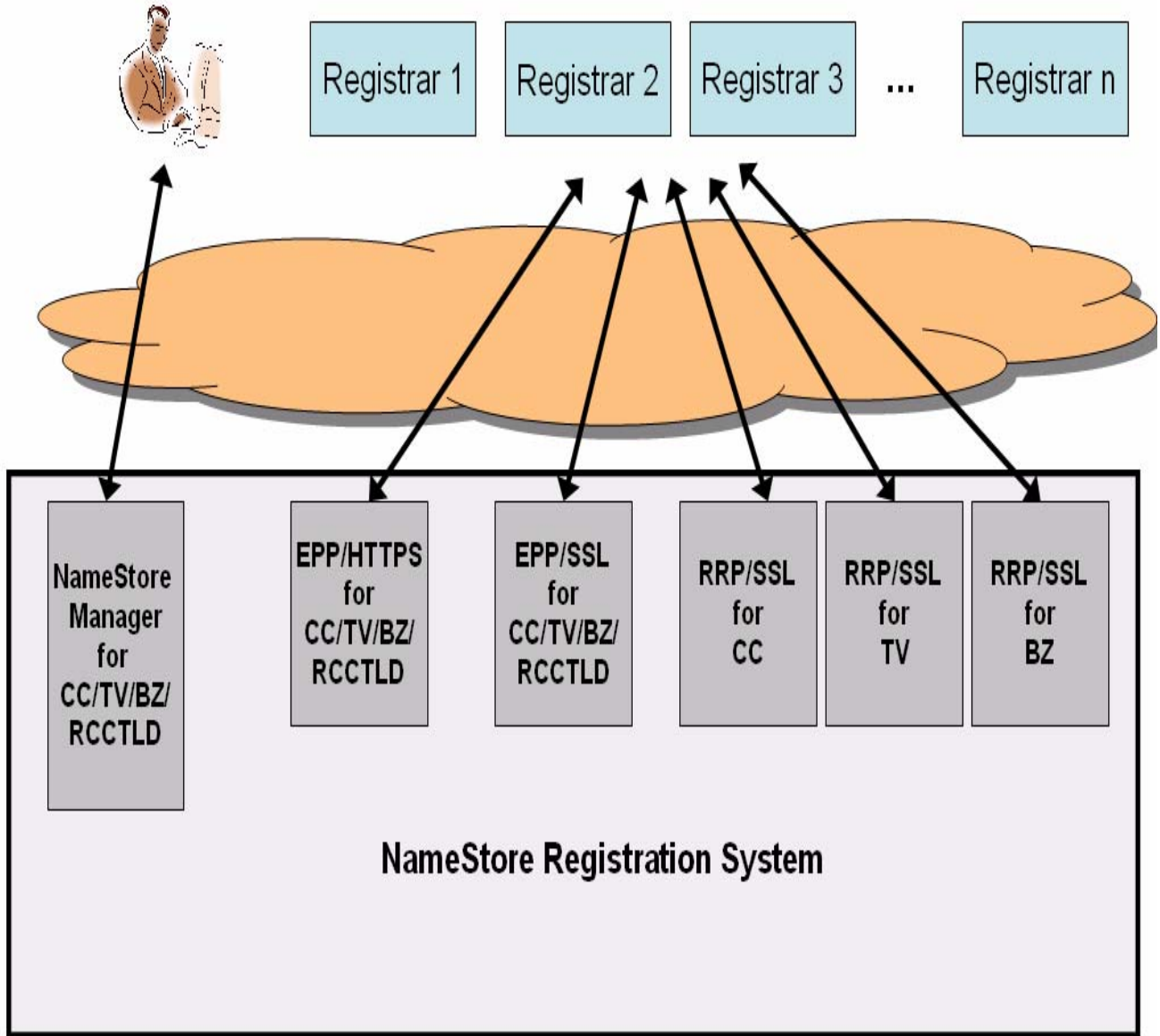
3. Name Store Access by Registrars

Registrars can access the online registration system in one of three ways for business to business communications via the following:

1. **EPP/SSL** - EPP (Extensive Provisioning Protocol) over TCP/SSL (Secure Socket Layer) Name Store gateway
and/or
2. **RRP/SSL** - RRP (Request Response Protocol) over TCP/SSL mechanism Name Store gateway
and/or
3. **EPP/HTTPS** - EPP over HTTPS (Hyper Text Transport Protocol using SSL) Name Store gateways

There is also a fourth approach for registrars to access Name Store registration system. This is achieved via a web based tool called Name Store Manager. It is primarily meant for manual access by the registrars.

The following diagram illustrates describes the registrar access the Name Store registration system:



4. Best Practices for Accessing RRP/SSL

A registrar interested in accessing the Name Store registration system service using the RRP protocol can achieve this by using RRP protocol over the TCP/IP based SSL protocol. In order to support RRP/SSL, a separate RRP/SSL gateway exists for each of the supported TLDs or products (CC, TV and BZ).

Since, each one of the RRP server runs on a separate VIP (Virtual IP)/port combinations, the registrars must open and maintain a separate connection for each product.

Also, since opening a connection is expensive, especially an SSL based session, registrars are encouraged to open a connection, login and hold on to the connection for performing subsequent RRP operations.

If no requests are processed by a connection within a certain amount of time, the connection may be terminated by the RRP Name Store gateway. This idle connection timeout has been set to 10 minutes (600 seconds).

An authenticated connection is subject to an idle timeout policy by the Name Store gateways. In order to prevent the authenticated connection from timing out a registrar can send an RRP DESCRIBE command to the Name Store gateway. We recommend that the registrar send the RRP DESCRIBE command only when necessary.

An authenticated connection also has an absolute timeout policy. The absolute timeout is defined as the longest period an authenticated session can be open for performing operations. This value is set to 24 hours. Registrars should disconnect, then reconnect and re-authenticate to resume RRP operations prior to the 24 hour timeout. We recommend that registrar's use the RRP Quit command and close the mature TCP connections cleanly and reconnect rather than letting it forcefully die when the time has expired.

For achieving maximized parallelism, a registrar may want to open multiple connections, login in and perform several RRP operations in parallel. We recommend that registrars use some sort of connection pooling mechanism in their software to achieve this parallelism. The maximum number of connections that a registrar can open across all channels is 15.

The downside to accessing the RRP/SSL Name Store gateway for registration is that it uses a unique VIP/port for each of the supported TLDs or products and thus will require a separate connection pool per TLD.

5. Best Practices for Accessing EPP/SSL

A registrar interested in accessing the Name Store registration system service using the EPP protocol can achieve this by using EPP protocol over the TCP/IP based SSL protocol. In order to support EPP/SSL, a single EPP/SSL gateway exists for all the supported TLDs or products (CC, TV, BZ and RCC).

Since there is a single Virtual IP (VIP)/port combinations for EPP/SSL Name Store gateway, the registrars can open and maintain a single connection for all of the supported TLDs or products.

Also, since opening a connection is expensive, especially an SSL based session, registrars are encouraged to open a connection, login and hold on to the connection for performing subsequent EPP operations.

Similar to the RRP Name Store gateway, if no requests are processed by a connection within a certain amount of time, the connection may be terminated by the EPP Name Store gateway. This idle connection timeout is set to 10 minutes (600 seconds).

An authenticated connection is subject to a timeout policy by the Name Store gateways. In order to prevent the authenticated connection from timing out, a registrar can send an EPP HELLO command to the Name Store gateway. We recommend that the registrar send the EPP HELLO command only when necessary.

An authenticated connection also has an absolute timeout policy. The absolute timeout is defined as the longest period an authenticated session can be open for performing operations. This value is set to 24 hours. Registrars should disconnect, then reconnect and re-authenticate to resume EPP operations prior to the 24 hour timeout. We recommend that registrar's use the EPP Logout command and close the mature TCP connections cleanly and reconnect rather than letting it forcefully die when the time has expired.

For achieving maximized parallelism, a registrar may want to open multiple connections, login in and perform several EPP operations in parallel. We recommend that registrars use some sort of connection pooling mechanism in their software to achieve this parallelism. The maximum number of connections that a registrar can open across all channels is 15.

The advantage to using EPP/SSL over RRP/SSL Name Store registration gateway is that there is a single VIP/port for all of the supported TLDs or products. Thus, registrars do not have to create a separate connection pool per TLD. Moreover, this is a standard registration protocol supported by the IETF.

6. Best Practices for Accessing EPP/HTTPS

A registrar interested in accessing the Name Store registration system service using the EPP protocol can also achieve this by using EPP protocol over the TCP/IP based HTTPS transport. In fact, this was the only supported connection that was available until this release. In order to support EPP/HTTPS, a single EPP/HTTPS gateway exists for all the supported TLDs or products (CC, TV, BZ and RCC).

The HTTPS transport is handled by sending XML data to Name Store inside an HTTPS POST message, where the HTTP headers have to be written to the secure socket before writing the XML data.

In this transport, the first message sent to the server should always be an HTTP GET. This will cause the server to return an EPP Greeting with a session cookie in the header (JSESSIONID). The session cookie should be included in subsequent HTTP POST commands as an HTTP header. This will let the server know that a greeting has already been returned to the client and that a conversation exists. "Content-Length" is the number of OCTETs in the message-body that is sent. This doesn't include the header.

Since there is a single Virtual IP (VIP)/port combinations for EPP/HTTPS Name Store gateway, the registrars can open and maintain a single connection for all of the supported TLDs or products.

HTTP is traditionally a connectionless protocol. However, since establishing a connection is expensive, especially an SSL based session, registrars are required to open a connection, login and hold on to the connection for performing subsequent operations.

Failure to do so may result in registrar privileges revoked.

Similar to the other two Name Store gateways, if no requests are processed by a connection within a certain amount of time, the connection may be terminated by the EPP Name Store gateway. This idle connection timeout is set to 10 minutes (600 seconds).

An authenticated connection is subject to a timeout policy by the Name Store gateways. In order to prevent the authenticated connection from timing out, a registrar can send an EPP HELLO command to the Name Store gateway. We recommend that the registrar send the EPP HELLO command only when necessary.

An authenticated connection is also subject to a time to live policy by the Name Store gateways. Time to live is defined as the longest period an authenticated session can be open for performing operations. This value is set to 24 hours. Registrars should disconnect, then reconnect and re-authenticate to resume EPP operations prior to the 24 hour timeout. We recommend that registrar's close the mature connections cleanly and reconnect rather than letting it forcefully die when the time has expired.

For achieving maximized parallelism, a registrar may want to open multiple connections, login in and perform several EPP operations. We recommend that registrars use some sort of connection pooling mechanism in their client software to achieve this. The maximum number of connections that a registrar can open across all channels is 15.

7. Managing Connections for Requests Related to RccTLD

In order to effectively use the Name Store platform, we recommend that registrars that are selling RccTLD in addition to CC TV or BZ manage a separate set of connections for the RccTLD commands. It is expected that response time for RccTLDs will be higher than CC TV or BZ since VeriSign relies on the external ccTLD registries to provide the response.

8. SSL Certificates

Every Registrar must use a 128 bit client certificate from VeriSign or Thawte in order to successfully establish a connection to the Name Store gateways. The Name Store gateways contain a list of trusted Certificate Authorities (CA) certificates. The client's certificate is checked when the client establishes a socket connection to verify that the certificate was signed by one of the trusted CA certificates. If the client's certificate was

not signed by one of these CA certificates, then the client connection is immediately closed. Also if a certificate is revoked by the CA it will not be allowed to connect.

The Name Store application verifies that the logon name and password are indeed correct, and that the IP address and SSL certificate x.509 certificate holder **common name** are listed in the system for the specific registrar issuing the EPP login or RRP session operation.

To summarize the SSL requirements, all Name Store interfaces as of December 14th in production and Sept 23 in OTE will be the following:

Interface	Number of Bits	Purpose of Certificate	Certificate Vendors
EPP/SSL RRP/SSL EPP/HTTPS	40/128	client or server	Verisign or Thawte

Note previous interfaces and their certificate requirements

Interface	Number of Bits	Purpose of Certificate	Certificate Vendors
Com/net (CORE)	40 or 128	client or server	Verisign or Thawte
Name Store .05 EPP/HTTPS	40 or 128	Server	Verisign
Name Store 1.0 EPP/HTTPS	128	Server	Verisign

9. Conclusion

The Name Store registration system offers a variety of choices for a registrar for domain names order processing. It is essential that the registrar follow the best practices outlined in this document for an effective, high performance and reliable business to business communication.