CenturyLink Technology Solutions

CenturyLink Technology Solutions Service Guide

SSL Certificate 1.0:

SSL Certificates

This Service Guide ("SG") sets forth a description of the SSL Certificate 1.0: SSL Certificates Service ("Service") offered by CenturyLink, including technical details and additional requirements or terms. This SG is subject to and incorporated into the Agreement and Hosting Service Schedule between the parties. The specific details of the Service ordered by Customer will be set forth on the relevant Service Order. For avoidance of doubt, any references in the Agreement, Schedules, or Service Orders to SSG,

Version	Previous	Section Modified	Date
HOS-20140730-SG-SSLCertificates	HOS-20140430-SG-SSLCertificates	Reformat	July 30, 2014

Table of Contents

Service Description 3

Tables and Appendices 5

Table 1.0 Roles and Responsibilities 5

Definition 6

Service Description

1. **Standard Service Description:** SSL Certificate 1.0: SSL Certificates ("Service" or "SSL Certificate Service") consists of the licensing, installation, administration, maintenance and support for the supported certificates listed in Section 1.1.1 Customer is responsible for choosing the SSL Certificate(s) that supports their requirements for securing information. This Service is not associated with a Service Level Agreement (SLA).

   1.1. Service Components: The SSL Certificate service provides nine options of commercially available SSL Certificates listed in Section 1.1.1 below each designed to provide site security based on Customer's needs, all with up to 256-bit encryption strength.

   1.1.1. **Supported Certificates**

   1.1.1.1. Symantec Secure Site Pro with EV (Extended Validation)
   1.1.1.2. Symantec Secure Site Pro
   1.1.1.3. Symantec Secure Site
   1.1.1.4. Thawte SLL Web Server with EV (Extended Validation)
   1.1.1.5. Thawte SSL Web Server
   1.1.1.6. Thawte SGC Super Cert
   1.1.1.7. Geotrust True BusinessID Wildcard
   1.1.1.8. Geotrust True BusinessID
   1.1.1.9. RapidSSL Certificate
   1.1.1.10. Geotrust Quick SSL Premium

   1.2. Licensing: CenturyLink provides the licenses in compliance with the certificate vendor licensing terms and conditions. Specific information on each vendors licensing terms and conditions can be provided on request. All users of the service are subject to the terms and conditions of the referenced license agreement.

   1.3. Installation: CenturyLink will provide installation tasks marked with an "X" in the CenturyLink column in Table 1.0 Roles and Responsibilities on the supported Operating Systems and Hosting Platforms listed below. Customer selects the operating system and platform at the time of purchase.

   1.3.1. **Supported Operating Systems:**

   1.3.1.1. Red Hat Enterprise Linux AS5 version 5.x (64 bit)
   1.3.1.2. Red Hat Enterprise Linux AS6 version 6.x (64 bit)
   1.3.1.3. Microsoft Windows Server 2003 R2
   1.3.1.4. Microsoft Windows Server 2008
   1.3.1.5. Microsoft Windows Server 2008 R2
   1.3.1.6. Microsoft Windows Server 2012

   1.3.2. **Supported Hosting Platforms:**

   1.3.2.1. CenturyLink Cloud: Only supports Geotrust, Quick SSL Premium
   1.3.2.2. CenturyLink Dedicated Cloud: Supports all certificates in section 1.1.1, with the exception of Geotrust, Quick SSL Premium.
   1.3.2.3. Intelligent Hosting: Supports all certificates in section 1.1.1, with the exception of Geotrust, Quick SSL Premium.

   1.4. Configuration: CenturyLink will provide setup tasks marked with an "X" in the CenturyLink column in Table 1.0 Roles and Responsibilities.

   1.5. Administration: CenturyLink will provide administration tasks marked with an "X" in the CenturyLink column in Table 1.0 Roles and Responsibilities.

1.5.1. **Public Assessment:** The Service utilizes automatic scanning protocols specific to each SSL Certificate service offering to conduct consistent assessment of public-facing web pages, web-based applications, server software, and network ports.

1.5.2. **Vulnerability Reporting:** Each SSL Certificate with built-in vulnerability assessment capabilities produces an actionable report that identifies both critical vulnerabilities that should be investigated immediately and informational items that pose lower risk.

1.5.3. **Malware Scanning:** SSL Certificates with daily malware scanning capabilities produce alerts for Customer to review for fast removal of malicious code and viruses.

1.6. Maintenance and Support: CenturyLink will provide maintenance and support tasks marked with an "X" in the CenturyLink column in Table 1.0 Roles and Responsibilities.

1.6.1. **Maintenance Windows:** All times listed under Schedule Maintenance Windows are local times and subject to change. CenturyLink will use commercially reasonable efforts to perform routine maintenance only during the Saturday or Sunday defined maintenance windows. See Definitions for additional information.

1.6.2. **Support**: Support for the Service is provided through the project manager during installation and Customer validation. At the point of go-live the Service is passed from project management to CenturyLink Service Center for full 24x7 monitoring and management. The point of go-live is when Customer notifies CenturyLink project manager that the environment is ready to go-live.

2. Customer Responsibilities: Customer is responsible for all tasks marked with an "X" in the Customer column in Table 1.0 Roles and Responsibilities. Customer acknowledges and agrees that its failure to perform its obligations set forth in Table 1.0 may result in CenturyLink's inability to perform the Services and CenturyLink shall not be liable for any failure to perform in the event of Customer's failure.

2.1. Certificate Selection: Customer is responsible for choosing the SSL Certificate that best aligns with their specific need based on securing information transfer between User and Site, distinguishing the varying levels of minimum encryption options available, scalable level of validation, and any extended validation available for additional credibility.

2.2. Provide Contact: Designate and maintain a Customer Contact during the Service Term (including current contact information). "Customer Contact" means a technical point of contact available 24 x 7 with sufficient knowledge, authority and access to address configuration issues, event notifications, system or infrastructure modifications and authentication of applicable CenturyLink systems.

3. Additional Services: Customer can choose to have CenturyLink complete one or more of the tasks in Table 1.0 with an "X" in the Customer column. The tasks can be added to the standard Service (described in Section 1.0) for an additional fee described in a Statement of Work ("SOW") and agreed to by the parties. Contact a sales representative for additional information.

Tables and Appendices

Table 1.0 Roles and Responsibilities

Activity	Task	CenturyLink	Customer
Licensing	Procure SSL Certificate	X	
Installation	Provide detailed requirements prior to Certificate request	X	
	Generate Certificate request		X
	Submit Certificate request to the vendor	X	
	Process Certificate request through vendor	X	
	Obtain Certificate from vendor	X	
	Provide Customer with a copy of the Certificate (when requested)	X	
	Install SSL Certificate on CenturyLink managed server	X	
	Install SSL Certificate on customers server		X
Configuration	Configure CenturyLink managed application with SSL Certificate	X	
	Configure Customer managed application with SSL Certificate		X
Administration	Initiate Certificate renewal request		X
	Initiate Certificate revocation request		X
	Perform Certificate revocation	X	
Support	Track the renewal date of the certificate and renew it as needed throughout the Service term	X	

Definition

Daily Website Malware Scanning: The malware scanning services scans website code for malicious software or codes that compromise Customer website data security. This service scans website code located at the hostname used in the SSL certificate and completes a static analysis of website code as well as behavioral analysis through a browser simulation to find code that may be activated by display of a page. Malware scanning reviews an optimal number of pages to identify and provides an instant alert when malicious code is identified to enable prompt removal.

Extended Validation (EV): Extended Validation represents the best, recommended type of certificate at the highest level of authentication using validation criteria as defined by the certification authority/browser forum. EV triggers web browser address bars to turn green and display the organization's name plus the issuing certification authority resulting in more security and more online trust for Customer sites.

Geotrust Quick SSL Premium: A basic domain encryption certificate.

Geotrust True BusinessID Wildcard: A certificate with full organization validation that covers an unlimited number of hostnames on an unlimited number of servers

Geotrust True Business ID: A certificate with full organization validation

RapidSSL Certificate: A basic and inexpensive certificate

Service Level Agreement: A service-level agreement (SLA) is a document describing the level of service expected by a customer from CenturyLink, laying out the metrics by which that service is measured, and the remedies or penalties, if any, should the agreed-upon levels not be achieved.

Statement of Work: A statement of work (SOW) is a formal document that captures and defines the work activities, deliverables, and timeline a vendor must execute in performance of specified work for a client. The SOW usually includes detailed requirements and pricing, with standard regulatory and governance terms and conditions.

Symantec Secure Site Pro with EV: An extended validation certificate with full organization validation, daily website malware scanning, weekly vulnerability assessments and SAN certificate support.

Symantec Secure Site Pro: A full organization validation certificate with daily website malware scanning, weekly vulnerability assessments and SAN certificate support.

Symantec Secure Site: A full organization validation certificate with daily website malware scanning, weekly vulnerability assessments and SAN certificate support.

Thawte SLL Web Server with EV: An extended validation certificate with full organization validation and SAN certificate support.

Thawte SSL Web Server: A certificate with full organization validation and SAN certificate support.

Thawte SGC Super Cert: A certificate with full organization validation

Vulnerability Assessment: Vulnerabilities are identified as potential entry points through which a website's functionality or data can be damaged. A vulnerability assessment provides an automatic weekly scan of public-facing web pages, web-based applications, and server software and network points.