

**CLICKSHARE SERVICE CORP.
PROVIDER AGREEMENT**

INFORMATION NEEDED TO OBTAIN SSL SERVER DIGITAL CERTIFICATE

This document is available from the Clickshare website as:

<http://www.clickshare.com/sales/Form-newCSP5-SSL.pdf> or
<http://www.clickshare.com/sales/Form-newCSP5-SSL.doc>

Q: When does a Clickshare Service Provider need a digital certificate?

If you wish to accept credit cards as a form of payment for online subscriptions or for article or multimedia content, you must obtain a special form of security for your website – an SSL Digital Certificate. Banks require that any website accepting credit-card numbers must use "Secure Sockets Layer" (SSL) encryption. This requires that your site obtain an "SSL certificate." Use this Clickshare explanation and data-form submission to start the process.

Q: What is a digital certificate?

A: A digital certificate is a small file which resides on a computer which serves web pages. Inside the file is a sequence of characters and some identifying information. The random sequence of characters is a code which is unique to the file -- and therefore to the computer on which it resides. That code can be used in a process called "Public Key Encryption" ("PKI") to encode and encrypt messages sent from the computer -- and unscramble or decrypt messages received by that computer. The identifying information is unique tied to the code sequence. The result of this setup is that web servers communicating with the machine that has the digital certificate can have a high degree of confidence that they are communicating with the machine whose owner is named in the associated identifying information.

Q: Why would my company want a digital certificate?

A: It is a requirement of accepting credit cards across the Internet. Web sites which want to accept credit card numbers use digital certificates, and the associated programs which use them, to allow consumers to send their credit-card number across the Internet with the numbers scrambled. This reduces the chance of fraudulent theft of credit-card numbers during their transfer. The digital certificates which Clickshare recommends work with the Secure Sockets Layer (SSL) encryption protocol which is common to web browsers supplied by Microsoft and Netscape to consumer computers. By obtaining and installing a digital certificate on your company's server, you are able to accept credit-card numbers in the most common and secure fashion. Most credit-card issuers will not process Internet credit-card transactions handled in any other way.

Q: Who issues digital certificates?

A: There are several vendors of digital certificates. Clickshare recommends and has a joint marketing relationship with Thawte (USA), Inc., which is a subsidiary of VeriSign Corp. Your company will pay Thawte an annual fee, and will receive a digital certificate -- file containing a unique alpha-numeric sequence identifying you machine so that you can accept credit cards at your web site. Clickshare typical pays the fee (\$159.00) and bills you.

Q: Who obtains the digital certificate?

A: Clickshare can obtain the digital certificate in your behalf, with your written authorization. The certificate will be owned by your company and will contain information about your company. We can act as your agent to obtain it, and to install it, if you wish, on a Clickshare-managed machine which is hosting your user-management services. Our you can install it on machines which you control directly.

CONFIDENTIAL / PROPRIETARY

Q: What information does Clickshare need to obtain the digital certificate for your company?

A: We need the information requested in the table below. Please complete it and return it by fax to 413-458-8002 or by email to support@clickshare.com.

Clickshare recommends Thawte (USA), Inc., a subsidiary of Verisign, Corp., for your server SSL certificate. For Thawte’s explanation of the need, see: <http://www.thawte.com/html/RETAIL/ssl/index.html>.

The steps Clickshare will undertake for you are described in an Enrollment Guide from the Thawte website at: <http://www.thawte.com/guides/StepByStepEnrollmentSSLSGC.pdf>

WHAT CLICKSHARE WILL DO

- ❖ Clickshare will apply for the digital certificate on your behalf. We will:
 - Step 1: Gather supporting documentation from you (below)
 - Step 2: Complete Thawte’s online application for you
 - Step 3: Pay the fee for the certificate, and bill you (approx. U.S. \$150.00)
 - Step 4: Make sure Thawte processes the request (3-5 business days)
 - Step 5: Clickshare will retrieve and install your certificate

WHAT YOU NEED TO DO

- ❖ You need to gather the following information in order for Clickshare to request your certificate. Use this form, and fax it to 413-458-8002, attention: Clickshare Certificate Administration. Confirm to your Clickshare representative by phone or email when you have faxed it. The Corporate Contact Person named below will receive a telephone call from Thawte requesting that Proof of Organization (such as an IRS or state-generated form) -- and a phone bill for the Corp Contact Number -- be faxed to Thawte.

SSL Secure Web Server Certificate Signing Request (CSR) information		
Country		
State (full name)		
City		
Company Legal Name		
Form of co ownership (circle)	Reg'd. Charity Private Company Reg'd. Non profit Government dept NGO Other	Sole Proprietorship Public Company (Listed) University Faculty admin University Dept Interest Group
Street Address of Org Head Office		
Department (optional)		
Server host (hostname)		
Admin email address		
A challenge password		
Corp Contact Person (non tech)		
Phone number		
Email address		
Job Title		