
Entrust.Net

**Technical Information –
Frequently Asked Questions (General)**



Client Confidential

© Entrust Technologies, 2000

Table of contents

GENERAL SERVER ISSUES.....	3
WHAT WEB SERVERS ARE SUPPORTED FOR ENTRUST.NET WEB SERVER CERTIFICATES?.....	3
WHY CAN'T I GENERATE A CSR?.....	3
WHY IS MY CERTIFICATE NOT WORKING?	3
HOW DO I BACK UP MY PRIVATE KEY?.....	3
I'VE LOST MY PRIVATE KEY, WHAT DO I DO NOW?	3
HOW DO I MOVE MY CERTIFICATE FROM ONE SERVER OR ISP TO ANOTHER?	4
WHY DO NAVIGATOR 3.X USERS SEE A "CERTIFICATE AUTHORITY EXPIRED" MESSAGE WHEN THEY CONNECT TO MY SERVER?.....	4

GENERAL SERVER ISSUES

This section provides the answers to the most commonly asked questions about supported Web servers. If you have a question that is not answered here please contact Entrust support.

WHAT WEB SERVERS ARE SUPPORTED FOR ENTRUST.NET WEB SERVER CERTIFICATES?

Entrust.net Web server certificates can be used with the Web servers listed in the table below. These Web servers all generate CSRs in a format that is recognized by Entrust. See valid certificate request formats for more information about CSR formats.

- Apache (mod_ssl)
- Apache-SSL
- C2Net Stronghold
- Microsoft Internet Information Server
- Netscape Enterprise Server
- O'Reilly WebSite Professional 2.x

WHY CAN'T I GENERATE A CSR?

You may have skipped a step in the CSR generation process described in the documentation that came with your Web server. Entrust also provides instructions for all the Web servers we support. See Instructions for generating CSRs for details. If your Web site is hosted by an ISP or virtual hosting company, then that organization will have to generate keys and CSRs on your behalf.

WHY IS MY CERTIFICATE NOT WORKING?

If you are having trouble using the certificate you received from Entrust, please read the Frequently Asked Questions for your server type. The most common problems are documented there.

HOW DO I BACK UP MY PRIVATE KEY?

It is very important to back up the private key that corresponds to the certificate you received from Entrust. Without the private key the Web server is unable to establish an SSL session. Each supported server has a different method of backing up the key. Consult your server documentation for details on how to back up the private key.

I'VE LOST MY PRIVATE KEY, WHAT DO I DO NOW?

If you lose your private key or it becomes corrupt and you do not have a backup, you will have to generate another key pair and CSR and request a new Entrust.net Web server certificate.

HOW DO I MOVE MY CERTIFICATE FROM ONE SERVER OR ISP TO ANOTHER?

To move your certificate from one ISP to another you must ensure that:

1. The domain name of your server at the new ISP matches the domain name in your certificate.
2. You can export your private key from your current ISP.
3. You can import your private key into the new server.

If any of the steps above are not possible you will have to request a new Entrust.net Web server certificate. If the steps above are all possible you may be able to transfer your certificate. Contact the ISPs involved for instructions.

WHY DO NAVIGATOR 3.X USERS SEE A “CERTIFICATE AUTHORITY EXPIRED” MESSAGE WHEN THEY CONNECT TO MY SERVER?

The root certificate included in Netscape Navigator 3.x expired in July 1998. Users of these browsers have two choices: they can upgrade to Netscape Navigator version 4.0 or higher which contains a root certificate that is valid until December 31, 2020; or they can import the new root certificate. Please see Root certificate rollover for a discussion of this issue.