



Brocade PKICERT Utility – Solaris Release Notes

May 2, 2003

Copyright © 2003, Brocade Communications Systems, Incorporated.

ALL RIGHTS RESERVED.

BROCADE, the Brocade B weave logo, Brocade: the Intelligent Platform for Networking Storage, SilkWorm, and SilkWorm Express, are trademarks or registered trademarks of Brocade Communications Systems, Inc. or its subsidiaries in the United States and/or in other countries. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners.

FICON[®] is a registered trademark of IBM Corporation in the US and other countries.

Notice: The information in this document is provided “AS IS,” without warranty of any kind, including, without limitation, any implied warranty of merchantability, noninfringement or fitness for a particular purpose. Disclosure of information in this material in no way grants a recipient any rights under Brocade's patents, copyrights, trade secrets or other intellectual property rights. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use.

The authors and Brocade Communications Systems, Inc. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

Notice: The product described by this document may contain “open source” software covered by the GNU General Public License or other open source license agreements. To find-out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit <http://www.brocade.com/support/oscd>.

Export of technical data contained in this document may require an export license from the United States Government.

TABLE OF CONTENTS

Overview	4
Important Notes.....	5
Secure Fabric OS	5
Installation.....	6
Other Important Notes.....	6
Outstanding Defects	6

Overview

PKI Certificate Installation Utility (for Solaris)

PURPOSE:

The main purpose of the PKI Certificate Installation utility is to provide functions that support automated installation of digital Certificates onto multiple switches.

INSTALLATION:

An environment variable, 'LD_LIBRARY_PATH=/usr/gnu/lib:...', must be defined that includes the path to the library files that accompanied pkicert, 'libFabOsApi.so' and 'libstdc++.so'.

USAGE:

This utility may be used interactively via its "text-based", "menu-driven" interface or it may be used from the command line. The command-line (batch mode) usage exists to support use of its functions from a script.

The easiest way to use this utility is to run it interactively by running the executable, 'pkicert' with no task-option arguments. An argument of -h prints the brief command line usage information. You can read more detailed help information by starting it with no command-line arguments and interactively choosing Help from the main menu.

The PKI-Certificate utility always writes event and error information to a log file, by appending or creating a new one if none exists.

You must provide IP addresses or switch names (domain aliases) of one switch in each fabric you want to access. The utility will operate on all switches in a fabric. You can not target a single switch in a multi-switch fabric.

Addresses or switch names can be provided in a file (one address or name per line) or manually entered as prompted.

Data files, both input and output contain switch data in XML format. You may view the data files with an editor, but do not attempt to edit them as this may invalidate the format or data.

This utility may be run from the command line. This is useful when using a script from which to run the pkicert utility.

Command (or 'batch') mode usage is as follows:

```
pkicert [task-options] [-e event-log-file] [-d data-file] [-a addr-file]
        [-A switch-addr] [-L log-level] [-u user-name -p password]
```

Task-Options:

- g Get CSRs & generate a CSR data file
- G Get CSRs (even from switches with certificates)
- i Install Certificates from a data file
- l Licensed Product report compile & generate

Event-Log-file: -e event-log-file

"event-log-file" is the path/file-name of log file created and written to (or if it already exists, appended to) with event/error data.

Data-file: -d data-file

"data-file" is the path/file-name of an input or output file

- * If the task-option is Get-CSRs, the file is an output file created and written to with CSR data.
- * If the task-option is Install Certificates, data is read from it.
- * If the task-option is Licensed Product report generation, the file is written to.

Address-file: -a addr-file

"addr-file" is the path/file-name of optional input file containing IP addresses or aliases of fabrics to which sessions should be established. If this argument is not provided, this data is read from the file indicated by environment variable 'FABRIC_CONFIG_FILE' if defined.

Address-Switch-IP: -A switch-addr

IP address of switch/fabric to which to connect for the given task.

Log-Level: -L n

"n" is a numeric value 0-3 indicating level of detail for information logged to the event log file. This may be provided on the command line using the '-L' argument while still using interactive mode. This is used primarily for debug purposes. Values and their meanings are as follows: 0 = silent; 1 = Error only; 2 = Events + Errors; 3 = Debug-info + Events + Errors.

Username: -u user-name

"user-name" is the login used for the one switch IP/Name given with the "-A switch-name" argument. If -u is used, a password must also be provided via the -p argument.

Password: -p password

"password" is the password that goes with the "-u user-name" provided.

Important Notes

Secure Fabric OS

The Secure Fabric OS is a comprehensive security product, which requires some planning and specific steps to set up and configure. For this purpose, the following documents should minimally be reviewed prior to getting started:

- *Secure Fabric OS Quick Start Guide*
- PKICERT and SecTelnet BETA Cheatsheets

More detailed product information may be obtained from the *Secure Fabric OS Users Guide*.

Installation

An environment variable, 'LD_LIBRARY_PATH=/usr/gnu/lib:...', must be defined that includes the path to the library files that accompanied pkicert, 'libFabOsApi.so' and 'libstdc++.so'.

Other Important Notes

This table lists important information you should be aware of regarding PKICERT.

Area	Description
Certificate load process	NOTE: Certificate load process should be run for 20 or less fabrics at the same time from pkiCert. If more than 20 fabrics should go through the process, request should be broken into batches of 20 or less fabrics.
Pkicert prompt	NOTE: While answering y/n questions for pkicert prompt, 'y' is taken as yes and all other characters are taken as no for an answer by default.
Switch names	NOTE: Switch names with spaces in it are not supported by Brocade website for issuing certificate. If requesting a certificate, switch name must be one word and should not contain spaces.

Outstanding Defects

This table lists open defects for PKICERT Utility v1.0.5.

Outstanding Defects		
Defect ID	Severity	Description
DEFECT000022811	High	<p>Summary: CSR retrieval from mixed fabric (with v4.1/non v4.1 OS) with mixed certificate (some with and some without): fails on retrieve on from switches with no certificates</p> <p>Symptom: If the customer has 1 or more Silkworm 3900 switches running Fabric OS4.0.x in a fabric with 1 or more other switches running 4.1.x, PKICert may fail to retrieve CSRs from some switches in that fabric that do not have certificates installed unless the user says CSRs should be retrieved even from switches that have certificates installed.</p> <p>Customer Impact: Customer should answer 'y' option to the question "Get CSR from switches even with certificates" in a mixed fabric environment. A fix is being considered for a future release.</p> <p>Probability: Medium</p>

Outstanding Defects		
Defect ID	Severity	Description
DEFECT000020957	Medium	<p>Summary: XML file generating in PKICERTutility which has blank spaces in the switch name will not pass through the website. Customer should be aware of this.</p> <p>Symptom: Switch name with blank spaces is supported on the switch, but DNS does not identify such names. Certificate for a switch with blanks in its name will not be accepted at Brocade website.</p> <p>Customer Impact: If requesting a certificate, switch name must be one word and should not contain spaces.</p>
DEFECT000022687	Medium	<p>Summary: pkicert test 2.2.1.6: retrieve CSR from multiple fabric with different (non-default) passwd, login prompt requires clarification.</p> <p>Symptom: When the wrong login/password is given which must be re-entered, only the WWN of the switch is provided not the switch name or IP address.</p> <p>Solution: This problem has been improved by having the WWN of the principal switch in the fabric be shown when the user is prompted for login and password. The API version used in this version of PKICert does not allow any other information about a fabric to be obtained until after logging into it.</p> <p>Customer Impact: A fix is being considered for a future release.</p> <p>Probability: Medium</p>
DEFECT000022893	Medium	<p>Summary: pkicert does not check and/or enforce for valid input</p> <p>Symptom: When asked a yes or no question, the user is prompted to enter 'y' or 'n', but anything other than 'y' is treated as if 'n' were entered.</p> <p>Solution: Now, only 'y' or 'n' are accepted when the prompt asks for "...(y/n)" and if multiple characters are entered at the prompted none carry over to the next prompt.</p> <p>Improper answer to Yes or No question is now rejected and user is prompted again</p> <p>Customer Impact: User should input valid y/n response.</p>

Outstanding Defects		
Defect ID	Severity	Description
DEFECT000023242	Medium	<p>Summary: Win2k/NT Readme file doesn't display properly under NotePad utility. However it is OK with WordPad.</p> <p>Symptom: If customer opens Readme.txt file for installation instructions under Win2K/NT with NotePad editor, the file is unreadable. Customer is encouraged to use WordPad with this version.</p> <p>Customer Impact: Use Release Notes provided for installation instructions.</p>
DEFECT000023832	Medium	<p>Summary: PKICert (mfg) : The Mfg function of pkicert needs to have consistent command-line output,</p> <p>Symptom: No customer impact!</p>
DEFECT000024483	Medium	<p>Summary: If CSR file name has only 1 or 2 alpha characters, user gets an 'fopen library fault' and prompt "Abort, Retry, Ignore".</p> <p>Symptom: If customer enters a CSR output file with only 1 or two alpha characters (no XML extension), the PKICERT program will get an 'fopen library fault' and prompt the customer "Abort, Retry, Ignore".</p> <p>Solution: The code did require that a filename have 3 characters (not including the ".xml" extension) now it can have just 1</p> <p>Workaround: File name should always be >= 3 characters excluding .xml extension</p> <p>Customer Impact: Customer should be advised to use file name greater than or equal to 3 characters excluding .xml extension.</p> <p>Probability: Medium</p>
DEFECT000025547	Medium	<p>Summary: PKICert Utility failed to create xml file after getting CSRs from 23 fabrics on NT and Win2k.</p> <p>Symptom: Certificate load process cannot be run for more than 20 fabrics at the same time.</p> <p>Solution: Program should be modified to handle more than 20 fabrics at the same time. This release limits maximum number of fabrics at 20.</p> <p>Workaround: If more than 20 fabrics are required to go through a certificate load, process should be broken in batches of 20 or less fabrics.</p> <p>Customer Impact: Certificate load process for more than 20 fabrics is not supported in this release.</p> <p>Probability: Low</p>

