Brocade PKICERT Utility - Solaris

Brocade OEM Final Disclosure Notes

Brocade Proprietary and Confidential Information

This document is intended for Brocade partners only.

May 2, 2003

TABLE OF CONTENTS

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	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 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. 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. Probability: Medium

Outstanding Defects		
Defect ID	**Severity**	**Description**
DEFECT000020957	Medium	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. 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. Customer Impact: If requesting a certificate, switch name must be one word and should not contain spaces.
DEFECT000022687	Medium	Summary: pkicert test 2.2.1.6: retrieve CSR from multiple fabric with different (non-default) passwd, login prompt requires clarification. 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. 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. Customer Impact: A fix is being considered for a future release. Probability: Medium
DEFECT000022893	Medium	Summary: pkicert does not check and/or enforce for valid input 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. 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. Improper answer to Yes or No question is now rejected and user is prompted again Customer Impact: User should input valid y/n response.

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

Cumulative Defects Closed To Date Since Beta 1

This table lists defects that have been closed since Beta 1.

Cumulative Defects Closed to Date Since Beta 1		
Defect ID	**Severity**	**Description**
DEFECT000012673	High	Summary: pkicert beta4_rc9 experiences segmentation fault when loading security certificates Symptom: pkicert will crash when using address file to input fabric IP addresses Solution: Address file input should be correctly read by the utility
DEFECT000022686	High	Summary: PKI SVT: Manufacturing PKICert Fails on Timeout Requirement Symptom: the application takes minutes to return from a situation where it can't get open a connection to the CS Solution: Added functionality for timeout and retry that is settable via config file name/value entries.
DEFECT000022850	High	Summary: MAX_N_SWITCHES variable not obeyed and also causes DEBUG Error flag and program exit. Symptom: the application does not stop getting CSRs when it has dealt with a number of switches equal to MAX_N_SWITCHES, but keeps going and crashes. Solution: Problem fixed. The parameter is not customer configurable.
DEFECT000022855	High	Summary: pkicert (Solaris) core dumps while retrieving CSR Symptom: If the user sets the configurable parameter MAX_N_SWITCHES too low and tries to deal with more switches than the number to which it was set, then the application would often crash. Solution: Removed MAX_N_SWITCHES from the list of configurable parameter. It now is set according to the largest number of switches found among the fabric to which communications sessions are established. The minimum value of MAX_N_SWITCHES is 10.
DEFECT000022886	High	Summary: PKI SVT: SLA Failed - Certificate turn-around time is too long Symptom: This is already fixed and Customer will no longer see this issue. Comment: IT has modified the processing logic at Brocade website to speed up the processing of large requests.

Cumulative Defects Closed to Date Since Beta 1		
Defect ID	**Severity**	**Description**
DEFECT000023737	High	Summary: PKI SVT: PKICert in Manufacturing Mode doesn't have retry Symptom: No customer impact. Solution: Retry happened but message were not printed. Solution is to print the messages. Workaround: None Comment: Fixed in this Release.
DEFECT000009553	Medium	Summary: PKICert gets CSRs for all switches in the fabric when it's told not to Symptom: No customer impact. Solution: Process user input correctly
DEFECT000009598	Medium	Summary: Unable to retrieve CSR from or install Certificate to switches without default password using pkicert (PC/NT version) Symptom: Customer will not be able to login using Windows version.
DEFECT000018351	Medium	Summary: When there is no CSR in the switches, the pkicert utility should give the right information Symptom: Customer may see wrong message. Solution: Newer versions of the utility display correct information message.
DEFECT000019833	Medium	Summary: Solaris: PKICert gets Segmentation Fault if it fails to write to .xml file Symptom: pkicert crashes if write permission is denied for the CSR file. Solution: Handle the file open error and display appropriate error message
DEFECT000021396	Medium	Summary: Need different pkicert for the customer who does not have the factory option Solution: Separate versions of pkicert for factory and customers are implemented.
DEFECT000022688	Medium	Summary: PKICert: CSR output file screen, dumps non-printable characters Symptom: In some screens, instead of a build-version number, there are some non-printable characters shown Solution: Correction to the way version number variable is provided.

Cumulative Defects Closed to Date Since Beta 1		
Defect ID	**Severity**	**Description**
DEFECT000022693	Medium	Summary: PKICert: test 2.2.1.:unable to retrieve CSR from two fabrics with different and non-default passwords Symptom: The message to users about getting no CSRs from a fabric did not clearly describe which fabric. Solution: Message improved to describe events without indicating Error
DEFECT000022714	Medium	Summary: Usability issue: User message for switches using non-standard passwords is misleading to customer Symptom: It was not clear from the message that the user had 5 tries to get the login/password info entered correctly Solution: Defaults for login and password are no longer used. Each Fabric WWN is shown (that's the only info available on fabric before login) at time of prompt for login and password.
DEFECT000022724	Medium	Summary: Usability issue: Path name management for Win2k/NT users is misleading Symptom: When asked for the name of a data file, if the user entered a file path & name that included non-existent folders/directories these are not created. Solution: Removed "Path/" from "... Path/filename ..."
DEFECT000022756	Medium	Summary: Unable to perform multiple retrieve operations in the same PKICert session Symptom: User had to restart PKICert to generate CSRs for different fabrics from those already entered. Solution: Menu navigation control was reworked by making significant changes to code structure and logic.
DEFECT000022809	Medium	Summary: Usability: CSR retrieval failure of non-v4.1 switches needs better user information/bogus status code Symptom: When a user tries to get CSRs from a fabric that includes switches running FOS version that does not support Fabric Security, the message for each such switch did not give switch name nor clear error info. Solution: Improved the information output to user when CSR get fails so it's better formatted and gives firmware version of the offending switch

Cumulative Defects Closed to Date Since Beta 1		
Defect ID	**Severity**	**Description**
DEFECT000022816	Medium	Summary: pkicert failed to retrieve CSR from the next fabric if all switches in the first fabric already have certificate installed Symptom: pkicert failed to retrieve CSR from the next fabric if all switches in the first fabric already have certificate Solution: Handle the option entered by user correctly to get certificates from switches which do not have certificates.
DEFECT000022817	Medium	Summary: Clarify error messages so it is clear to user that pkicert is behaving correctly and as expected. Symptom: CSRs are retrieved from all switches regardless of whether there are certificates installed or not. Solution: No error message appears now if user specifies that CSRs are not to be obtained from switches with certificates installed and a fabric has only switches with certificates installed. Now when no CSRs are retrieved because all switches already had certificates, the information is clear and does not indicate an error.
DEFECT000022821	Medium	Summary: Add (Optional) to question in PKICert: "Include licensed product data (y/n)?" Symptom: The message asking whether user wants Licensed product data included with their CSR file, it did not say that the licensed product information is optional. Solution: Added "(optional)" to question "Include licensed ..."
DEFECT000022828	Medium	Summary: Usability: Harsh error message delivered when XML file name is either missing or is illegal (also comes late!) Symptom: When an invalid data file name is provided by the user, a message appears saying "Error: failure getting valid file name..." Solution: Changed the messages to say "Sorry, a valid file name is required to proceed"
DEFECT000022848	Medium	Summary: Supplying bad or misspelled DNS name for CSR probe causes program to abruptly exit with no error messages Symptom: Supplying bad/misspelled DNS for CSR fabric address causes program to quit abruptly. Supplying a non-existent IP address string tends to "hang" the user interface too long and also eventually quits. Solution: Made sure the user is returned to the main menu when this situation occurs. There is now a meaningful message and the user is returned to the main menu.

Cumulative Defects Closed to Date Since Beta 1		
Defect ID	**Severity**	**Description**
DEFECT000022853	Medium	Summary: pkicert.exe vs. pkicert executable have different program behavior access of config file (and other issues) Symptom: None, there is no noticeable change in behavior. Solution: Remove configuration file
DEFECT000022856	Medium	Summary: Customer .xml files should not be overwritten by default Symptom: When asked for a CSR (output) data file name, if a user enters the name of an existing file, it will be overwritten without warning. Solution: If a file by the same name already exits, the user is warned and can change output data file name. Or go ahead and overwrite the file. Appending to an existing file is not an option.
DEFECT000022889	Medium	Summary: PKI SVT: CA server Core Dump Symptom: Customer will not get certificate within specified period on website. Solution: This is reassigned to PKI team for resolution and being tracked.
DEFECT000022895	Medium	Summary: PKICert does not check for proper setup of PKICERT_CONFIG_FILE env var (Solaris) Symptom: Customer might have set an environment variable with the Config file name, but it wouldn't get used. Solution: Use of config file was eliminated. New command line options allow user to specify Log-Level and event-log file name, etc.
DEFECT000022900	Medium	Summary: .XML extension is not assumed or tried on reading supplied certificate filename for download to a fabric Symptom: If a certificate input data file name is given without an extension, the application does not assume that an extension of ".xml" was left off and should be added. Solution: If no file name extension is given, ".xml" is now appended before asking user for approval
DEFECT000022905	Medium	Summary: Win2k/NT attempt to save certificate report to bad path causes assert failure in fprintf.c - and program dies Symptom: If user gives a data file name with an invalid path (non-existent directory/folder) then the application would crash. Solution: Do not close unopened file. fclose was being called with NULL file pointer.

Cumulative Defects Closed to Date Since Beta 1		
Defect ID	**Severity**	**Description**
DEFECT000022921	Medium	Summary: General Usability: Clarify or expand cryptic tags, e.g., (1/5) for retries, variables like #fabs, etc. Symptom: When a wrong switch login/password must be re-entered, the fact that this was try # 1 of 5 was displayed as (1/5), which may not make sense to most users. Solution: Improved information format output to user
DEFECT000022922	Medium	Summary: Generating report: Need to print out (repeat) stored report location in output screen when saved and also precheck. Symptom: After generating a License report, the report file name was not repeated on the screen Solution: License report file name is clearly shown after it has been written to report file name. And is now given at the end of the license report generating process
DEFECT000022923	Medium	Summary: Usability: Customers prefer in-situ logging for MS-DOS window applications to external log file Symptom: Customer can't scroll the screen because this is a console application. Solution: Interactive logging is not possible with current design of application. This can be fixed by creating a GUI application.
DEFECT000023094	Medium	Summary: Solaris install of pkicert needs PKGADD capability for common admin installs Symptom: Customer needs to be experienced enough to set up all the parameters for using pkicert in a Solaris environment. pkgadd command is not presently available for pkicert. Solution: Add pkgadd capability