Aladdin eToken PKI Client ReadMe
Version 5.1 SP1 Revision A
Release Date: January 2010

==

This document contains last minute information about eToken PKI Client 5.1 SP1.

We recommend reading the *eToken PKI Client 5.1 User's Guide* and the *eToken PKI Client 5.1 SP1 Administrator's Guide* before implementing the solution.

Note: Documentation is provided in pdf format. You must install Adobe Reader to read the pdf documents. Adobe Reader can be downloaded from www.adobe.com

Contents

1. Support

We work closely with our reseller partners to offer the best worldwide technical support services. Your reseller is the first line of support when you have questions about products and services. However, if you require additional assistance you can contact us directly:

Telephone

You can call our help-desk 24 hours a day, seven days a week:

USA: 1-800-545-6608

International: +1-410-931-7520

Email

You can send a question to the technical support team at the following email address:

support@safenet-inc.com

Website

You can submit a question through the SafeNet Support portal:

http://c3.safenet-inc.com/secure.asp

2. Licensing

The use of this product is subject to the terms and conditions as stated in the End User License Agreement.

3. Default eToken Password

Tokens are shipped from our factory with the default eToken Password 1234567890. The end user must enter this default password the first time s/he logs on to eToken, and then change it to a secure personal password.

4. Supported Platforms

eToken PKI Client 5.1 SP1 supports the following operating systems:

- Windows XP SP3/SP2 (32-bit and 64-bit)
- Windows Vista SP2 (32-bit and 64-bit)
- Windows 7 (32-bit and 64-bit)
- Windows Server 2003 SP2 (32-bit and 64-bit)
- Windows Server 2008 (32-bit and 64-bit)
- Windows Server 2008 R2

5. Languages

The following languages are supported:

- Chinese (Simplified)
- English
- French (European)
- French (Canadian)
- German

- Italian
- Japanese
- Korean
- Polish
- Portuguese (Brazilian)
- Russian
- Spanish
- Thai

6. Installation

For more information, refer to the eToken PKI Client 5.1 SP1 Administrator's Guide.

- Install eToken PKI Client 5.1 SP1 using the full MSI installation, or use the MSP package on top of an already installed eToken PKI Client 5.1
- eToken PKI Client 5.1 SP1 MSP installation supports installation upgrades for eToken PKI Client 5.1 only
- eToken PKI Client 5.1 SP1 MSI installation supports installation upgrades for eToken PKI Client 4.0 and higher only
- All previous installation properties are supported
- New properties can be passed to the installation via the command line PROP_REG_FILE
  This property provides the path to a registry file:
  c:\>msiexec /i PKIClient-x32-5.1-SP1.msi PROP_REG_FILE ="C:\path to registry file.reg" /qb
  (where PKIClient-x32-5.1 is the appropriate 32- or 64-bit installation file)
  For more details about the PRO_REG_FILE registry key, refer to the *eToken PKI Client 5.1 SP1 Administrator's Guide.*

7. New Features in eToken PKI Client 5.1 SP1

eToken PKI Client 5.1 SP1 introduces support for the following features:

- **Support for more Microsoft platforms:** Supports Windows 7 and Windows Server 2008 R2, Internet Explorer 8.0
- **Support for more token devices:** Supports the flash partition application on eToken NG-Flash 4.50 CardOS, eToken NG-Flash 5.30 Java, and eToken NG-Flash 5.30 Java Anywhere devices
- **Support for more hash algorithms:** Supports the SHA-2 family of algorithms
- **TolerantX509Attributes:** Default changed to enable the use of certificates created in a non- DER-encoded binary x.509 format
- **More dependable:** Resolves customer-reported issues from earlier releases

8. New Features in eToken PKI Client 5.1

eToken PKI Client 5.1 introduces support for the following features:

- **Improved Remote Desktop Access:** Supports Remote Desktop access with Windows Server 2008

- **Service Pack Mechanism Support:** Supports the Service Pack upgrade method for easy implementation of future support and maintenance features
- **Non-ASCII Character Support:** Supports non-ASCII characters in the authenticator password used for Smart Card logon
- **Support for eToken PRO Anywhere GA:** For use as a standard eToken Pro in the enterprise

9. Updates and Resolved Issues in eToken PKI Client 5.1 SP1

This section lists issues resolved in the eToken PKI Client 5.1 SP1 release.

ID	Description	Solution/Workaround
19951	When connecting with a smart card to Windows Server 2008 via Remote Desktop, if the smart card removal behavior was configured on the server to lock the workstation, if the eToken was removed without closing the RDP session, when the eToken was re-inserted it was not possible to enter the session.	Fixed
20068	Calling a hardware random number generator (RNG) with two tokens connected, causes the following error message to be displayed: "The operation requires a Smart Card, but no Smart Card is currently in the device"	Fixed
20096	When logging on over a Remote Desktop Connection some slowness occurred randomly.	Fixed
20161	When the user attempted to connect to Windows Server 2008 through Remote Desktop Connection, an error message was displayed and the PKI tray icon on the server side stopped responding.	Fixed
20163	When attempting to generate a sub MS CA certificate to a token, the process sometimes fails and an error message is displayed.	Fixed
20431 21087	After upgrading eToken PKI Client, the Smartcard Logon certificate was no longer set as the default. The customer was required to log on manually, and set the certificate to default in eToken Properties.	Fixed

ID	Description	Solution/Workaround
20591	After connecting to a remote computer through Remote Desktop Connection using a Smartcard Logon certificate logon, when the token was removed the remote computer was not locked, even though the GPO had been set to activate this feature.	Fixed
20592	WSO 3.0 caused an excessive amount of CPU usage.	Fixed
21381	Cisco VPN with SBL did not work with eToken PKI Client 5.1, as the Cisco VPN Client was not directed correctly to the certificate.	Fixed
21442	If a user connected to a Citrix terminal session with Smart Card logon (eToken PKI Client 5.1 and eToken Pro), the terminal session stopped responding. If the user then removed the token, the terminal session began responding, but the session closed.	Fixed
21459	Sometimes, when using a PFX file with a long name, no information was displayed in the "Issued to" field in eToken Properties.	Fixed
21460	When working with Entrust Entelligence Security Provider (EESP) 7.1 and Smart Card Logon with an MS CA certificate, after attempting to perform a key recovery the MS CA certificate was orphaned.	Fixed
21636	eToken Properties, running on Windows XP 32-bit, sometimes stopped responding.	Fixed

ID	Description	Solution/Workaround
21682	Sometimes, import of a PFX file onto a computer running Windows Vista failed with the following error message "Failed to acquire context".	Fixed
21749	TolerantX509Attributes enabled by default	Fixed.
21783	Running Certutil.exe with the –Scroots parameter on Windows Vista failed.	Microsoft known issue
21845	In some rare instances, when attempting to enroll a token, an error was displayed indicating a password complexity error, even though the complexity was set to zero.	Fixed
21957	When signing a PDF using a token in a Citrix ICA session, if an attempt was made to sign multiple documents during the same application session, the second attempt at signing caused eToken PKI Client to stop responding, until the token was removed.	Fixed
22005	When several tokens are connected to a computer running Windows Vista, an assertion error occurred when a token was removed.	Fixed
22006	Sometimes, when attempting to close eToken Properties by clicking on the window close button, the application stopped responding and displayed the following error message: "The memory could not be read".	Fixed

ID	Description	Solution/Workaround
22075	When a user used Internet Explorer to access an SSL page, using a certificate on the token, if the token was then removed from the computer and re-inserted after the SSL session had terminated (but the IE session was still running), a message was displayed that the site needed a certificate to log on. The expected behavior was for the user to be prompted to re-enter the password.	Fixed
22124	Previously, support PKCS#11 CKM_SHA256/SHA384/SHA512 mechanism was not supported.	PKCS#11 CKM_SHA256/SHA384/SHA512 is supported
22163	When attempting to connect using Citrix ICA after the second attempt the session stopped responding. When the token was removed, the session started responding.	Fixed
22212	There were some textual errors in the Russian localization of eToken PKI Client.	Fixed
22023	Sometimes, eToken PKI Client displayed the amount of free memory on the token incorrectly. If the token was used directly through the Application Protocol Data Unit (APDU), and not by eToken PKI Client, the value of the remaining bytes could be modified without eToken Properties being updated, resulting in the wrong value being displayed in eToken Properties.	Fixed

10. Updates and Resolved Issues in eToken PKI Client 5.1

This section lists updates and resolved issues in eToken PKI Client 5.1..

ID	Description	Solution/Workaround
16664	If the eToken was removed during the initialization process and an error occurred, reinserting the eToken will cause the eToken Properties Application to terminate with an error.	Fixed
19218	When working with Minidriver, it is not possible to log on to an eToken if the password has expired or if the "must change password feature" is activated."	The password can be changed using eToken Network Logon or on a computer where eToken PKI Client is installed.
19156	Previously, when the rename eToken function was disabled (by setting the registry key HKEY_LOCAL_MACHINE\ SOFTWARE\Aladdin\eToken \MIDDLEWARE\AccessControl to zero) the function was disabled only in the Simple view. It was still possible to change rename the eToken in the advanced view.	Fixed
19149	In Windows Server 2008, it was possible to log on with only one eToken at a time.	Fixed
18314	eToken PKI is unexpectedly terminated when working with certain Smart Card readers.	Fixed
18015	The Windows Event Viewer sometimes reported an error following the initialization of eTokens.	Fixed
17955	eToken PKI is unexpectedly terminated when removing an eToken.	Fixed

ID	Description	Solution/Workaround
19754	When using single-sign-on, the user should be required to log on for the first logon process only. New or existing processes should not require an additional log on. If the token is removed and re-inserted, only the first process should require a password for log on. In previous versions of eToken PKI Client, each process required a password.	Fixed
19566	When upgrading from earlier versions of CLM and eToken RTE 3.65 to PKI 5.0 SP1 or later, there were errors dues to a difference in the manufacturer's ID. Manufacturer ID name changed to "Aladdin Knowledge Systems Ltd."	Fixed

11. Known Issues

This section lists known issues in the eToken PKI Client 5.1 and eToken PKI Client 5.1 SP1 releases.

ID	Description	Solution/Workaround
15261 Installation/ Upgrade	If eToken WSO 3.0 is installed on a computer with eToken PKI Client 5.0 or later installed, or vice versa, a message is displayed during the install process prompting the user to close eToken PKI Monitor process. However, there is no option to close the eToken PKI Monitor process.	Select ignore and re-boot after the installation.
16608 Installation/ Upgrade	If eToken PKI Client 5.0 or later and eToken WSO 3.0 are installed, and eToken WSO 3.0 is then uninstalled without saving the settings, all eToken PKI Client settings and readers are removed from the registry.	When uninstalling eToken WSO, select the option to keep the settings.
16729 Installation/ Upgrade	After upgrading to eToken PKI Client 5.0 or later from an earlier version, connected eToken Virtuals may be erroneously displayed as emulated.	To resolve this issue, do one of the following: Upgrade without saving settings (the eToken Virtual will be disconnected). Disconnect and reconnect the eToken Virtual
16188 Installation/ Upgrade	If eToken PKI Client is installed on the client computer via GPO, with the GPO installation configured as "assign", the eToken PKI Client tray icon does not appear, even though the eToken PKI Monitor process is running.	If you log off then log on again, the eToken PKI Client tray icon appears. The problem will not occur if the GPO installation is set as "publish."
16770 Installation/ Upgrade	When installing PKI Client 5.0 on Windows Vista, the installation sometimes stops with error 1935.	Restart the computer and restart the installation.
16126 Installation/ Upgrade	If the PKCS#11 Security Provider is added manually to Firefox and eToken PKI Client 5.0 or later is installed, the security provider will be installed twice (as the eToken PKCS#11 Security Provider is installed during the installation of eToken PKI Client 5.0). The user will be prompted to select the required Security Provider.	Manually remove the superfluous PKCS#11 Security Provider.

ID	Description	Solution/Workaround
16616 Installation/ Upgrade	If eToken PKI Client 5.0 or later and eToken WSO 3.0 are installed on the same computer and eToken PKI Client 5.0 or later is uninstalled, the eToken PKI Client tray icon does not show the eToken Properties menu item.	Launch eToken Properties from **Programs>eToken>eToken PKI Client >eToken Properties.** The installation repair process is launched, fixing the defect.
16772 Installation/ Upgrade	After upgrading from version 4.55, the eToken PKI Client tray icon does not appear and the PKI monitor process is not displayed in the Windows Task Manger.	Restart the computer.
16734 Installation/ Upgrade	Sometimes, the eToken PKI Client 5.0 or later installation does not add the PKCS#11 module to Firefox.	Before installing eToken PKI Client 5.0 or later, in Firefox open the Device Manager by selecting **Tools>Options>Advanced >Security Devices**. Click **OK.** This action adds the required configuration file, so if eToken PKI Client 5.0 or later is now installed, the PKCS#11 module is added to Firefox, as expected.
16839 Installation/ Upgrade	If eToken PKI Client 5.0 or later is downgraded to version 4.55 (by uninstalling version 5.0 and installing 4.55), the eToken Properties application does not run.	After uninstalling eToken PKI Client 5.0, remove the eTProps.exe file from the installation folder before installing version 4.55.
16771	In Windows Vista, after uninstalling eToken PKI Client 5.0 or later, the eTFS.dll file remains on the computer in the system32 folder.	
16789	When uninstalling eToken Properties through the command line, the eToken Properties menu item is not removed from the eToken PKI Client tray icon. (The menu item performs no action when selected).	

ID	Description	Solution/Workaround
13932	An EFS certificate cannot be created with the Microsoft basic template.	Microsoft has released a hotfix to deal with this issue. To obtain the hotfix, contact eToken support.
16369	Connecting to Microsoft VPN failed when two tokens we connected.	Microsoft is working on a solution. (Microsoft case SRQ080701600004.)
16373	Logon via Microsoft Smartcard logon or Microsoft VPN fails when using an eToken initialized with a secondary authentication RSA key.	
16726	When attempting to log on via Windows Remote Desktop Connection, with a smartcard logon certificate on a Flash device, the logon fails. This is because the Microsoft Terminal Service cannot recognize a USB flash memory device connected to the client computer.	
16694	It is not possible to download a Smart Card Logon certificate or a Smart Card User certificate via Firefox.	
16727	When a computer restarts from standby or hibernation mode, eToken Properties does not function correctly.	Click the eToken Properties refresh button.
16486	In Windows Vista, even if certificate propagation is disabled by changing the PropagateUserCertificates registry key to 0 (zero), certificate propagation might still occur.	Close the Microsoft Windows Vista Certificate Propagation Service.
16497	In some rare cases, when connecting to Check Point VPN, the authentication screen is not in focus for keyboard input. The user is required to click on the authentication screen to get it into focus.	

ID	Description	Solution/Workaround
16796	In eToken NG-Flash Partition Application, if the Help menu is selected, the documentation will not open if Adobe Reader is not installed on the computer. There is no message informing the user that Adobe Reader must be installed.	Install Adobe Reader.
16476	In Windows 64-bit, if you double-click the eToken Virtual (.etvp) or eToken Rescue (.etv) file, the token is not connected to eToken PKI Client.	To connect eToken Virtual or eToken Rescue in 64-bit systems, open eToken PKI Client Properties advanced view, select the **Tokens** node and click the **Connect eToken Virtual** icon**.**
16227	If an attempt is made to remove a non-deletable certificate from the certificate store by setting the registry key **RemoveFromTokenOnRemoveFromStore** to 1 (true), a message is displayed confirming that the certificate has been deleted, even though, as expected, it has not been deleted.	
17882	In Windows Vista, when working with OWA, when attempting to encrypt or sign with a private key, an error message "No digital ID found" is displayed, even though a valid certificate is present. This is a limitation of OWA when working with Windows Vista.	Disable protected mode in Internet Explorer by doing one of the following: • Go to **Internet Options > Security** and uncheck Protected Mode • To disable Protected Mode only for OWA, go to **Internet Options > Security > Trusted Sites>Add Site** and add the URL of the OWA site
19760	Clicking on **Delete eToken Content** while the **Change Password** or **Synchronize Password** dialog boxes are open causes the Change **Password** dialog box to stop responding.	Close the Change Password **dialog box.**
19797	When uninstalling eToken PKI Client from Windows Server 2008 or Windows Vista, a message is displayed prompting the user to close the eToken PKI tray icon or other application.	Click **Ignore** and continue uninstallation.

ID	Description	Solution/Workaround
19308	Sometimes, the eToken PKI tray icon might not display the connected eTokens correctly.	Re-insert the eToken(s).
19877	If eToken PKI Client is installed on a server while users are logged on via Remote Desktop (RDP), eToken PKI Client might not be installed correctly.	Verify that there are no open RDP sessions before installing eToken PKI Client.
20163	When attempting to generate a sub MS CA certificate to a token, the process sometimes fails and an error message is displayed.	Fixed
20702	During a Citrix multi-session (Where there is a smart card logon from a computer with a Citrix ICA client into a Citrix server, and the Citrix server is connected through a RDP session to another non-Citrix computer) the token is not recognized in the logon window.	For more information see the Public Citrix HotFix which is available from the Citrix Knowledge Centre (the latest version is included in HotFix Rollup Pack 04 for XenApp 4.5 / XenApp 5.0) See article CTX119069 for the HotFix, and the Readme (English) for Windows 2003 Server (see line item 26). Hot fix#197595 includes different language versions of the HotFix to resolve this behavior. Ensure that you use the appropriate version for your environment and HotFix level.
21967	When upgrading to eToken PKI Client 5.1 SP1, an error message indicates that the file is in use. This is a standard occurrence for an MSI installation.	Click Ignore and continue the installation.

ID	Description	Solution/Workaround
22161 20392	The eToken PKI Client Logon window stops responding when logging on to the Check Point VPN.	The workaround is: 1. Go to regedit > HKEY_LOCAL_MACHINE > Software > Aladdin > eToken > MIDDLEWARE > UI 2. Add new key - SR_Service.exe 3. Add new dword - RunExternalDialog with value data 1
22250	Sometimes, when logging on to RDP with Smart Card logon, the user is asked for both the token password and Windows logon credentials.	Re-insert the token and log on again to RDP.
22278	Sometimes, when connecting with multiple RDP connections to Windows Server 2008, sometimes the certificates were not visible in the certificate store.	Re-insert the token and unlock the station; the certificate becomes visible in the certificate store.

12. API Changes

This section describes changes to the API in the PKI Client 5.1 release.

.

DCR	Subject	Description
18785	**CAPI** CryptGetProvParam function	In eToken PKI Client 5.1 CryptGetProvParam the new Microsoft Crypt_Next flag is supported: • Multiple tokens connected. • CryptAquireContext with the following parameters: dwFlags = CRYPT_VERIFYCONTEXT, pszContainer = Null • Subsequent call of CryptGetProvParam with PP_ENUMCONTAINERS: o In Previous releases, information was returned for arbitrary selected token. o PKI 5.1 lists all containers of all the connected tokens.
19462	**PKCS#11** CKM_GENERIC_SECRET_KEY_GEN and CKM_RC4 mechanisms	eToken PKI Client 5.1 re-introduces support for CKM_GENERIC_SECRET_KEY_GEN and CKM_RC4 for tokens formatted with legacy formats (format 0 or 4).
19566	**PKCS#11** C_GetSlotInfo and C_GetTokenInfo	Manufacturer ID name changed to "Aladdin Knowledge Systems Ltd."