

eToken RTE README

Version 3.65

Release Date: January 2006

=====
This document contains general comments plus last minute notes from the eToken RTE 3.65 product team. The information in this README is more up to date than the product documentation.

The README document contains the following:

- [Getting Started](#): describes the scope of this document.
- [General Notices](#): lists the various support centers, details the end user license agreement and the default eToken password.
- [What's New?](#): provides information about new features and changes since previous versions of eToken RTE.
- [General Recommendations](#): presents a number of recommendations to be followed as a matter of common activity when working with the RTE and eToken.
- [Known Issues](#): lists the known issues when working with this version of eToken RTE.
 - [General Issues](#)
 - [Installation Issues](#)
 - [CAPI Application Issues](#)
 - [PKCS11 Application Issues](#)
 - [Driver Issues](#)

1. Getting Started

This document is designed to give administrators an understanding of what is new in eToken RTE 3.65. A variety of features have been added and improved for administrator convenience and an enhanced user experience.

The document also provides a quick reference for known issues that may occur while implementing or using this version of eToken RTE.

This document does not explain how to use or configure eTokens using eToken RTE. For information on how to prepare eTokens for specific security applications, refer to the documentation provided. We strongly recommend that you first read the manuals provided prior to implementing eToken authentication.

2. General Notices

2.1. Support

If you have any questions regarding this package, its documentation and content or how to obtain a valid software license you may contact your local reseller or Aladdin's technical support team:

Country / Region	Telephone
USA	1-212-329-6658 1-800-223-3494
EUROPE: Austria, Belgium, France, Germany, Netherlands, Spain, Switzerland, UK	00800-22523346
Ireland	0011800-22523346
Rest of the World	+972-3-6362266 ext 2

2.2. Licensing

Please note that the use of this package requires a valid software download license that will be emailed to you. Please first logon to the Aladdin license center www.Aladdin.com/lc and download the latest software and documentation that you have purchased. If you do not have a valid license to download, you should contact your reseller or support center. (The necessary support numbers are listed above)

2.3. Default Password

All eTokens are shipped from our factory with a DEFAULT PASSWORD (PIN) 1234567890. You will need to input this default password the first time you logon to eToken and then change it to your secret and secure personal password.

3. What's New

This section lists the new functionality provided by eToken RTE 3.65.

The new eToken RTE 3.65:

- Provides support for new tokens:
 - eToken devices with the CardOS 4.20B and 4.30B operating systems. These will include versions of the eToken PRO (32K and 64K) and eToken NG-OTP (32K and 64K).
These new tokens provide the user with better performance, more EEPROM and support for RSA 2048-bit cryptography.
- Provides better support in CAPI-enabled applications for keys and certificates that were created by PKCS#11-enabled applications.
- Supports the Supplementary API (SAPI) to eToken as introduced in SDK 3.60.
- Provides better integration of PKCS#11 keys through CAPI.

4. General Recommendations

- **Do not remove an eToken from the USB port during an operation.**
Many operations, such as key generation, certificate enrollment, certificate removal etc. require multiple actions with the eToken. If the eToken is removed during one of these actions, the data structure on the eToken may be damaged and data lost as a result. In such a case the eToken may need to be reinitialized.
- **Do not remove an eToken while multi-token initialization of other tokens is in progress.**
This may result in data loss or failure to initialize the removed eToken thus rendering it unusable.
- **When working remotely, such as via a Terminal Server, changes made on the eToken (enrollment and removal of certificates for example) may not be synchronized with locally running applications and vice versa.** It is therefore recommended to avoid modifying any eToken content under these conditions. If necessary however, it is recommended that the eToken is reinserted after such modifications are made.
- **If using an eToken to secure a Microsoft VPN connection and you use several eTokens, ensure that only the correct eToken is inserted when opening the connection and not several eTokens at the same time.** If several eTokens are inserted when starting the connection, the operating system asks you to choose the correct token. However Microsoft VPN does not pass your choice to the RTE and your operation may fail as a result of using the wrong eToken.
- **Do not initialize an eToken PRO 32K (CardOS 4.30) to work with 2048-bit RSA keys.** Although it is possible the eToken will work it is not recommended. There may be insufficient memory remaining on the eToken as the support module loaded onto the eToken is almost 16k alone.
- Only eToken PRO with CardOS 4.20 or later Operating System and eToken NG-OTP can be initialized with the HMAC or RSA 2048 support modules.

- An eToken 64K has a file size limitation and is therefore only able to create files on the eToken that are a maximum of 32K in size for each single file.
- It should be remembered that removing a certificate from the eToken (via eToken Properties) does not remove the copy of this certificate from the certificate store on the computer.

5. Known Issues

This section lists known issues in this release of eToken RTE.

- [General Issues](#)
- [Installation Issues](#)
- [CAPI Application Issues](#)
- [PKCS11 Application Issues](#)
- [Driver Issues](#)

5.1. General Issues

- Only users with Administrator privileges are able to change "Local Machine" options. Ensure that you have these privileges if you want to change parameters affecting Certificate Store Options, Power Saving Options or Readers Management.
- It may occur that the eToken has insufficient space to store both the certificate and key on it. In such a case, the error message that may appear depends entirely on the application being used. In some cases no error message appears and this may be confusing for the user experience.
- Some changes (like **Enable power saving**) only become effective after a reinsertion of the eToken. In certain cases, a message asking to reboot is displayed but not in all.
- Under Windows XP, when trying to use the RunAs functionality from the command line, you may experience a failure to read from the smart card reader. This failure is not related to the smartcard vendor, and will occur with or without eToken RTE installed, i.e. with eToken or any other smartcard vendor drivers.
- When working with eToken Properties and you attempt to import a certificate to the eToken either from the local computer store or from a PFX file, you receive an error message "Invalid handle". This message may be confusing and is due to the fact that MS Windows uses this error code for several possible failures, e.g. lack of free space on the eToken, attempting to import 2048-bit RSA keys to an eToken that does not support these keys, etc.
- If working in Windows 2000, ensure that the latest Service Pack is installed (SP 4 or later) if you try to import a p12 certificate file with a 2048-bit key either to the computer or to an eToken or the operation may fail.
- It is not recommended to use an eToken R2 when working with Citrix Metaframe as the eToken may fail.

- When working with Check Point Firewall, the removal of any inserted eToken will close the VPN connection, even if that eToken was not used for authentication to the VPN.
- An eToken initialized as a FIPS token is not supported by the Aladdin SAA SecuRemote application.
- Certain USB Smartcard Readers may have problems of various degrees working with the OS4 card. It is recommended that you contact the relevant reader vendor to obtain their latest software upgrade.
- RDC (Remote Desktop Connection) in the context of eToken usage means that a remote process on a remote computer can access the locally inserted eToken.
- Terminal Server – A session can be opened via modem, but in such a case transactions involving the token may work slowly. In order to improve such slow communications, the session will be opened in a “Read Only” mode.
- Previously the eToken PRO 16k version with an Administrator password might have returned an error when a 1024 bit RSA key is generated for a second time. To ensure this does not occur, initialize the eToken with the eToken initialization feature supplied with RTE 3.65.

5.2. Installation Issues

- On occasion the installation of the RTE may result in a rollback because of an installed antivirus (like Norton or another antivirus). Completely removing the antivirus program or configuring the antivirus to allow for copying files to the Windows directory will enable the user to install the RTE again.
- To install the RTE, the user must be a local administrator on that computer. Once installed the RTE can be used by anyone without local administrator privileges.
- When installing the RTE on Windows NT, the BIOS must be set to “USB Legacy Support – ON”.
- To ensure that an unexpected error from the Smartcard Resource Manager is not displayed during RTE installation, verify that the Outlook Express application is closed and the process msimn.exe is not running. If it is, end the process before continuing the installation.
- It is recommended that when installing RTE 3.65 on NT machines you do not insert an eToken during the installation process.
- On Windows NT and Windows 9x, the Resource Manager limits the number of Smart card readers both actual and virtual to 10.
- Installing the RTE on Windows Me may result in an error message during installation. Nevertheless, the RTE **does** work correctly after a system reboot.

5.3. CAPI Application Issues

- When closing Outlook Express under a Windows XP system, this process should end automatically. On occasion the process does not end automatically and this might

causes problems with future mail decryption. To solve this problem kill the Outlook Express (e.g. msimn.exe in the Windows Task Manager).

- When working on Windows NT with certificates stored on the eToken and going to IE->Tools->Internet Options->Content->Certificates, make sure that the certificate's friendly name is not too long. A long name will cause Internet Explorer to terminate itself with an error. To fix this change the 'friendly name' of the certificate (this is done by double-clicking on the certificate, and going to the 'Details' tab->Edit Properties->Friendly Name) and then making the 'friendly name' shorter.
- When importing a PFX/P12 certificate using the Import/Export Wizard the private key MUST be marked as exportable.
- Importing p12 files that were exported from an R2 token does not work and results in the following error message: "An internal error occurred. The private key you are importing might require a cryptographic service provider that is not installed on your system". However if you are using Netscape, this import process DOES work.
- A Smart Card certificate may not appear in the certificate list in Internet Explorer, until the computer is rebooted for the first time since installing the RTE.
- Aladdin recommends that smartcard logon certificates and smartcard user certificates from Microsoft CA should not be protected with secondary authentication.
- In certain cases, a user may encounter an error when trying to establish a VPN connection using PIX or Concentrator VPN. In such a case, the user should reboot the machine and this will solve the problem.
- When enrolling a Smartcard Logon Certificate on behalf of a different user with Microsoft CA, ensure that only one eToken is inserted during the process. If more than one eToken is inserted, the operation will fail. Depending on the platform in use, the error message may be confusing.
Only in the case where the Enrollment Agent certificate is located on a different eToken is it permissible to insert more than one eToken during the operation.

5.4. PKCS#11 Application Issues

- Some PKCS#11 applications (such as PGP or Mozilla) may not work properly if the token PIN is not initialized (in terms of PKCS#11). This may occur if the token was initialized with a previous RTE version or with unsuitable initialization parameters. For example, when creating an Entrust profile on an eToken with Administrator password, Entrust **will** change the Administrator password to a random password. To avoid this and similar problems, either initialize the eToken with proper parameters (which is done by default since RTE 3.60) or use the eToken Properties configuration tool to change the user password.
- CardOS versions prior to 4.20 do not support public exponent as an input parameter for RSA key generation. Applications that generate key pairs must export the public exponent (public key) after key generation. This is relevant for the eToken PRO family.

- From RTE 3.60, the PKCS#11 module is added automatically in Windows 2000 and Windows XP. For other operating systems, the user must add this module manually.
- Working with Netscape browser and two eTokens with the same eToken Label concurrently connected, cryptographic operations may not work. To solve this, remove one of the eTokens or set it with a different label.
- The RTE 3.65 installation adds the eTPKCS11.DLL to the Netscape Cryptographic Module database. This will not happen if Netscape does not have a user account. To solve this problem, initialize a Netscape user account and then repair the RTE. This will add the eTPKCS11.DLL to the Netscape database.
- Netscape browser versions up to 4.7x as well as version 7.1 and Mozilla browser version 1.7 are supported.
- Netscape does not read correctly eToken labels with more than one blank space in it. Please refrain from using eToken labels that contain more than one space.
- If you have two certificates with the same subject name on the eToken, this may result in a problem when attempting to enter a secure web site if using Netscape browser.
- If you use Netscape 7.1 for email ensure that you install a proper CA certificate in Netscape, otherwise if you sign your email with a certificate located on the eToken only, the application may fail and terminate abnormally.
- If installing Entrust, users must copy the entrust.ini file from the server to the client before installing the RTE. After this the RTE automatically adds the two eTPKSC11 lines to this file allowing for complete integration with Entrust.
- Lotus Notes requires the presence of only ONE SmartCard Reader. If more readers are connected Lotus Notes will not enable Smartcard Login for the application that is using the eToken.
- If after downloading a certificate using Netscape 4.76 and then deleting the certificate in Netscape, the user tries to delete keys via eToken Properties, the operation may fail. To avoid this situation, either use Netscape 7.1 or higher OR delete certificates and keys ONLY by using eToken Properties.

5.5. Driver Issues

- The USB stack for Windows NT installed with eToken RTE 3.65 supports only eToken devices. As a result, after installation of the RTE 3.65 there may be a conflict with other connected USB devices, for example it may use 100% of the CPU.
- When working with Windows NT 4.0, do not remove the eToken during initialization of a single eToken or remove an initialized eToken while multi-token initialization is still in progress as this may result in a system failure requiring a reboot.
- When working with Windows 98, the computer may not wake up from standby/hibernate mode if the eToken Properties management tool was left open before going into standby.