

SafeWord Authenticators



Copyright

© 2011 Aladdin Knowledge Systems Ltd. ("Aladdin"). All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without written permission from Aladdin.

Trademarks

Aladdin, SafeWord, PremierAccess, RemoteAccess, and SecureWire are trademarks of Aladdin. All other trademarks, tradenames, service marks, service names, product names, and images mentioned and/or used herein belong to their respective owners.

Software License Agreement

The following is a copy of the Software License Agreement as shown in the software:

CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE LOADING THE SOFTWARE. THIS AGREEMENT GOVERNS THE USE OF THE SOFTWARE (AS DEFINED BELOW). BY CLICKING "I ACCEPT" BELOW, OR BY INSTALLING, COPYING, OR OTHERWISE USING THE SOFTWARE, YOU ARE SIGNING THIS AGREEMENT, THEREBY BECOMING BOUND BY ITS TERMS. BY INDICATING YOUR AGREEMENT, YOU ALSO REPRESENT AND WARRANT THAT YOU ARE A DULY AUTHORIZED REPRESENTATIVE OF THE ENTITY THAT HAS PURCHASED THE SOFTWARE AND THAT YOU HAVE THE RIGHT AND AUTHORITY TO ENTER INTO THIS AGREEMENT ON THE ENTITY'S BEHALF. IF YOU DO NOT AGREE WITH THIS AGREEMENT, THEN CLICK "I DO NOT ACCEPT" BELOW OR DO NOT USE THE SOFTWARE AND RETURN ALL COPIES OF THE SOFTWARE AND DOCUMENTATION TO ALADDIN OR THE RESELLER FROM WHOM YOU OBTAINED THE SOFTWARE.

1. DEFINITIONS.

1.1 "Documentation" means the published user manuals, User Guide and any additional documentation that are made available for the Software.

1.2 "Software" means the machine-readable object-code version of Aladdin's SafeWord software including any revisions, corrections, modifications, enhancements, updates and/or upgrades thereto that you may receive.

2. GRANT OF LICENSE. Aladdin grants to you, and you accept, a personal, nonexclusive, non-transferable and fully revocable limited license to use the Software, in executable form only, for a predefined set number of licensed users, as described in the Software accompanying Documentation and only according to the terms of this Agreement. Under no circumstances will you receive any source code of the Software. Aladdin also grants to you, and you accept, a non-exclusive, and non-transferable limited license to use the Documentation solely in conjunction with the Software.

3. LIMITATION OF USE. You may not: 1) copy the Software, except to make one copy of the Software solely for back-up or archival purposes; 2) transfer, distribute, rent, lease or sublicense all or any portion of the Software or Documentation to any third party; 3) translate, modify, adapt, decompile, disassemble, or reverse engineer any Software in whole or in part; 4) modify or prepare derivative works of the Software or the Documentation; or 5) use the Software to process the data of a third party; 6) place the Software onto a server so that it is accessible via a public network; and 7) use any back-up or archival copies of the Software (or allow someone else to use such copies) for any purpose other than to replace an original copy if it is destroyed or becomes defective. You agree to keep confidential and use your best efforts to prevent and protect the contents of the Software and Documentation from unauthorized disclosure or use. Aladdin reserves all rights that are not expressly granted to you. If you are a member of the European Union, this agreement does not affect your rights under any legislation implementing the EC Council Directive on the Legal Protection of Computer Programs. If you seek any information within the meaning of that Directive you should initially approach Aladdin.

4. DISCLAIMER OF WARRANTIES. Aladdin does not warrant that the functions contained in the Software will meet your requirements or that operation of the program will be uninterrupted or error-free. The entire risk as to the results and performance of the Software is assumed by you. THE SOFTWARE IS FURNISHED, "AS IS" WITHOUT ANY WARRANTY OF ANY KIND, AND ALADDIN AND ITS LICENSORS HEREBY DISCLAIM ALL WARRANTIES, EXPRESS, IMPLIED OR STATUTORY IN RESPECT OF THE SOFTWARE INCLUDING, WITHOUT LIMITATION, ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES AS TO NON-INFRINGEMENT. SOME STATES AND COUNTRIES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS WHICH VARY BY STATE OR COUNTRY.

5. LIMITATION OF REMEDIES. ALADDIN'S AND ITS LICENSORS ENTIRE LIABILITY UNDER, FOR BREACH OF, OR ARISING OUT OF THIS AGREEMENT, IS LIMITED TO A REFUND OF THE PURCHASE PRICE OF THE SOFTWARE OR SERVICE THAT GAVE RISE TO THE CLAIM. IN NO EVENT SHALL ALADDIN OR ITS LICENSORS BE LIABLE FOR YOUR COST OF PROCURING SUBSTITUTE GOODS. IN NO EVENT WILL ALADDIN OR ITS LICENSORS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL, EXEMPLARY, OR OTHER DAMAGES INCLUDING, WITHOUT LIMITATION, ANY LOSS OR DAMAGE TO BUSINESS EARNINGS, LOST PROFITS OR GOODWILL AND

LOST OR DAMAGED DATA OR DOCUMENTATION, SUFFERED BY ANY PERSON, ARISING FROM AND/OR RELATED WITH AND/OR CONNECTED TO DELIVERY, INSTALLATION, USE OR PERFORMANCE OF THE SOFTWARE AND/OR ANY COMPONENT THEREOF, WHETHER OR NOT ALADDIN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

6. TERM AND TERMINATION. This license is effective until terminated. You may terminate it at any time by destroying the Software, including all computer programs and Documentation, and erasing any copies residing on computer equipment. This Agreement also will automatically terminate if you do not comply with any terms or conditions of this Agreement. Upon such termination you agree to destroy the Software and Documentation and erase all copies of the Software residing on computer equipment.

7. PROTECTION OF CONFIDENTIAL INFORMATION. The Software and Documentation are delivered to you on a confidential basis and you are responsible for employing reasonable measures to prevent the unauthorized disclosure or use thereof, which measures shall not be less than those measures employed by you in protecting your own proprietary information. You may disclose the Software or Documentation to your employees as necessary for the use permitted under this Agreement. You shall not remove any trademark, trade name, copyright notice or other proprietary notice from the Software or Documentation.

8. OWNERSHIP. The Software and Documentation are licensed (not sold) to you. All intellectual property rights including trademarks, service marks, patents, copyrights, trade secrets, and other proprietary rights evidenced by or embodied in or attached/connected/related to the Software and Documentation are and will remain the property of Aladdin or its licensors, whether or not specifically recognized or protected under local law. This License Agreement does not convey to you an interest in or to the Software, but only a limited right of use revocable in accordance with the terms of this license agreement. Nothing in this Agreement constitutes a waiver of Aladdin's intellectual property rights under any law. You will not remove any product identification, copyright notices, or other legends set forth on the Software or Documentation.

9. EXPORT RESTRICTIONS. You agree to comply with all applicable United States export control laws, and regulations, as from time to time amended, including without limitation, the laws and regulations administered by the United States Department of Commerce and the United States Department of State. You have been advised that the Software is subject to the U.S. Export Administration Regulations. You shall not export, import or transfer Software contrary to U.S. or other applicable laws, whether directly or indirectly, and will not cause, approve or otherwise facilitate others such as agents or any third parties in doing so. You represent and agree that neither the United States Department of Commerce nor any other federal agency has suspended, revoked or denied your export privileges. You agree not to use or transfer the Software for end use relating to any nuclear, chemical or biological weapons, or missile technology unless authorized by the U.S. Government by regulation or specific license.

10. U.S. GOVERNMENT RIGHTS. Any Software or Documentation acquired by or on behalf of a unit or agency of the United States Government is "commercial computer software" or "commercial computer software documentation" and, absent a written agreement to the contrary, the Government's rights with respect to such Software or Documentation are limited by the terms of this Agreement, pursuant to FAR § 12.212(a) and its successor regulations and/or DFARS § 227.7202-1(a) and its successor regulations, as applicable.

11. ENTIRE AGREEMENT. This Agreement is our offer to license the Software and Documentation to you exclusively on the terms set forth in this Agreement, and is subject to the condition that you accept these terms in their entirety. If you have submitted (or hereafter submit) different, additional, or other alternative terms to Aladdin or any reseller or authorized dealer, whether through a purchase order or otherwise, we object to and reject those terms. Without limiting the generality of the foregoing, to the extent that you have submitted a purchase order for the Software, any shipment to you of the Software is not an acceptance of your purchase order, but rather is a counteroffer subject to your acceptance of this Agreement without any objections or modifications by you. To the extent that we are deemed to have formed a contract with you related to the Software prior to your acceptance of this Agreement, this Agreement shall govern and shall be deemed to be a modification of any prior terms in their entirety.

12. GENERAL. Any waiver of or modification to the terms of this Agreement will not be effective unless executed in writing and signed by Aladdin. If any provision of this Agreement is held to be unenforceable, in whole or in part, such holding shall not affect the validity of the other provisions of this Agreement. By entering into this Agreement, you agree to allow Aladdin to obtain current license information from the system or systems on which the Software is installed for the purpose of determining license renewal information. You may not assign this License Agreement or any associated transactions without the written consent of Aladdin. This Agreement shall be construed and governed in accordance with the laws of Israel (except for conflict of law provisions) and only the courts in Israel shall have jurisdiction in any conflict or dispute arising out of this Agreement. The application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

Technical Support information

Aladdin works closely with our reseller partners to offer the best worldwide Technical Support services. Your Aladdin reseller is the first line of support when you have questions about products and services; however, if you require additional assistance, contact us directly.

- For all support related issues (product overview, training, downloads and documentation, and tech support contact information), see our Web page at: www.aladdin.com/sw-support.
- To use the Aladdin KnowledgeBase, go to www.aladdin.com/kb-sw. You will need to enter your Company ID to access knowledge base articles.

Publishing history

Date	Part number	Software release
January 2008	86-0948337-A	SafeWord Authenticators, all versions
June 2008	86-0948337-B	SafeWord Authenticators, all versions
October 2008	86-0948337-C	SafeWord Authenticators, all versions
October 2009	76-010100-B	SafeWord Authenticators, all versions
April 2010	76-010152	SafeWord Authenticators, all versions
July 2010	76-010184	SafeWord Authenticators, all versions
October 2010	76-010191	SafeWord Authenticators, all versions
April 2011	76-010213	SafeWord Authenticators, all versions
September 2011	007-011558-001	SafeWord Authenticators, all versions

About SafeNet and Aladdin Knowledge Systems

In 2007, SafeNet was acquired by Vector Capital, a \$2 billion private equity firm specializing in the technology sector. Vector Capital acquired Aladdin in March of 2009, and placed it under common management with SafeNet. Together, these global leading companies are the third largest information security company in the world, which brings to market integrated solutions required to solve customers' increasing security challenges. SafeNet's encryption technology solutions protect communications, intellectual property and digital identities for enterprises and government organizations. Aladdin's software protection, licensing and authentication solutions protect companies' information, assets and employees from piracy and fraud. Together, SafeNet and Aladdin have a combined history of more than 50 years of security expertise in more than 100 countries around the globe. Aladdin is expected to be fully integrated into SafeNet in the future. For more information, visit www.safenet-inc.com or www.aladdin.com.

CONTENTS

CHAPTER 1	Hardware Authenticator Overview	1
	Overview	2
	Authentication modes	2
	Synchronous authentication	2
	Asynchronous authentication	3
	SafeWord hardware tokens	4
	SafeWord Gold token	4
	eToken PASS token	5
	SafeWord Alpine token	5
	SafeNet 3300 token	6
	Traditional passwords	6
CHAPTER 2	Using Hardware Tokens	7
	eToken PASS tokens	8
	Alpine tokens	10
	Using Alpine tokens	11
	Using other SafeWord-supported tokens	12
	SafeWord Gold tokens	12
	SafeNet eToken 3300 (Platinum) tokens	14
	Programming tokens	17
	Programming Alpine tokens using Token Programmer Kit software	17
	Programming tokens using eToken Programmer software	18
	Assigning SoftPINs to tokens	18
	Deploying SafeWord-supported authenticators	19
	Index	21

CHAPTER
1

Hardware Authenticator Overview

In this chapter...

Overview	2
Authentication modes	2
SafeWord hardware tokens	4
Traditional passwords	6

Overview

This document discusses hardware authentication methods and modes supported by SafeWord. It includes details about each SafeWord hardware authentication option.

Authentication modes

SafeWord hardware tokens feature the following authentication modes

- Time or event (synchronous) authentication
- Challenge-response (asynchronous) authentication

Synchronous authentication

Synchronous authentication is not dependent on a challenge being issued by the SafeWord Authentication Engine. Instead, the Authentication Engine knows - from the imported token data file - the encryption algorithm being used by the tokens entered into the database, and what passcodes to expect from each token. The passcodes are synchronized between the Authentication Engine and the token using either time-dependent or event-dependent synchronization.

Time-synchronous mode

In time-synchronous mode, the one-time passcodes change automatically every 10 to 60 seconds. And since the SafeWord token clock continuously runs in the background, the passcodes are always in sync.

Event-synchronous mode

Event-synchronization uses an ordered passcode sequence to determine which passcode is valid. The Authentication Engine determines which passcode is valid by tracking where in the sequence of numbers a token should be. Synchronization can be maintained between the server and token even if the token is a few passcodes ahead of the server.

How synchronous authentication works

Synchronous authentication works as follows:

- 1 A user attempts to access a protected resource, and is prompted to enter their user ID and token-generated passcode.
- 2 The SafeWord Authentication Engine verifies that the received passcode is what was expected.
 - If the passcode is what was expected, access is allowed.
 - If the passcode is not what was expected, access is denied.

Since synchronous authentication does not require users to enter a challenge, the user workload is lighter. Also, nearly all authentication protocols can support synchronous tokens.

Asynchronous authentication

Asynchronous authentication uses a challenge-response system in which the SafeWord Authentication Engine issues a “challenge” to a user seeking access to a protected resource. The user enters the issued challenge into the token, which generates a single-use passcode response. Asynchronous authentication works as follows:

- 1 A user attempts to connect to a protected system by entering their user ID, and SafeWord responds by issuing a challenge to the user.
- 2 The user types the challenge into their token.

The token holds an encryption algorithm identical to that held by the SafeWord Authentication Engine. The token decrypts the challenge and displays a single-use passcode that will be expected by the Authentication Engine.
- 3 The user enters the token-generated passcode into the prompt, and the Authentication Engine verifies the passcode matches the expected response.
 - If the passcode matches the appropriate encryption code, the user is allowed access to that system.
 - If the passcode does not match the appropriate encryption, the user is denied access to that system.

SafeWord hardware tokens

SafeWord hardware tokens are hand-held passcode generators programmed to validate the passcodes. They have a liquid crystal display (LCD) to display their generated passcodes, and either a single button to generate a passcode, or a simple keyboard to enter SafeWord-issued challenges into the token.

SafeWord supports the following token types from SafeNet:

- SafeWord Gold
- eToken PASS
- SafeWord Alpine
- SafeNet eToken 3300 (Platinum)

SafeWord also supports tokens available from other vendors. For information on other vendors' tokens, contact SafeNet Technical Support.

SafeWord Gold token

The SafeWord Gold is designed in a key fob case design and works in either synchronous or asynchronous mode. It incorporates features including the option of a one-time passcode mode, a pre-expired PIN mode (forcing change of default PIN at first use), the option to set a fixed number of PIN uses, and more user-friendly display prompts.

Figure 1: SafeWord Gold token



eToken PASS token

The eToken PASS token is compact and portable, and provides strong user authentication to network resources from any computer, at any time. It features one-time passcode (OTP) generation with the press of a button. It features event-synchronous and time-synchronous authentication options, OATH compliance, and an on-off button to preserve battery life.

Figure 2: SafeWord eToken PASS token



SafeWord Alpine token

The SafeWord Alpine token generates highly secure one-time passcodes, ensuring properly authenticated access to critical applications and data. The Alpine token combines a compact design with a sturdy clip for convenient attachment. It features event-synchronous and time-synchronous authentication options, OATH compliance, and an on-off button to preserve battery life.

Figure 3: Alpine token



SafeNet 3300 token

SafeNet 3300 tokens are the top-of-the-line hardware tokens. They have the same features as the SafeWord Gold. The durable case and housing enables SafeNet 3300 SafeNet 3300 tokens to have the longest warranty available in the industry.

Figure 4: SafeNet 3300 token



Traditional passwords

SafeWord 2008 includes support for traditional fixed or memorized passwords. Some users may possess strong authentication devices, while others may use fixed passwords. Passwords failing to meet the administrator's requirements are rejected; these may include previously-used passwords.

CHAPTER
2

Using Hardware Tokens

In this chapter...

eToken PASS tokens	8
Alpine tokens	10
Using other SafeWord-supported tokens	12
Programming tokens	17
Deploying SafeWord-supported authenticators.....	19

eToken PASS tokens

The eToken PASS is a compact, portable one-time passcode (OTP) token that enables users to securely access network resources from any computer using strong two-factor authentication. Both event-synchronous and time-synchronous eToken PASS hardware tokens are available.

Figure 5: eToken PASS
token



eToken PASS options

eToken PASS option rules are defined by the administrator. These rules dictate which passcode(s) and password(s) must be provided by the user for authentication. The options are:

- OTP only - The user enters only the OTP value generated from the eToken PASS device.
- OTP and OTP SoftPIN- The user enters the OTP value generated from the eToken PASS device, and enters the OTP SoftPIN.
- OTP and Windows password - The user enters the OTP value generated from the eToken PASS device, and enters their Windows password.

Using eToken PASS tokens

When a user is prompted to authenticate to a protected resource, they simply press the button on the face of their eToken PASS, and a random OTP value is displayed. This value is the one-time passcode the user will enter into the password field of the challenge prompt. If this user has a SoftPIN assigned to their token, they must also append that SoftPIN to the passcode in order to authenticate.

Resetting the PIN

Both the administrator and the user can easily reset the eToken PASS PIN. The user can reset their PIN from the User Center, while the administrator resets PINs from the Active Directory User Center Management Console, or from the SafeWord 2008 Management Console.

Expiration of the eToken PASS

eToken PASS tokens never expire. Additionally, the battery life of the eToken PASS is 14,000 OTP generations (button clicks) over seven years, providing practically limitless operation.

Note: eToken PASS supports six (6) digit passcodes only.

Alpine tokens

SafeWord Alpine tokens come either pre-initialized and configured, or can be programmed using Token Programmer Kit Software. Pre-programmed tokens are shipped in the default programming mode unless you ordered customized Alpine tokens with optional settings.

Figure 6: SafeWord Alpine token



Customized Alpine tokens can be requested using SafeNet's Custom Token Programming Order Form. For more information about ordering Alpine tokens with customized options, please contact your SafeNet sales representative.

Pre-programmed Alpine token settings

The following is a list of the Alpine token programming settings. Default settings are indicated where appropriate.

1 Mode

The display mode of the token. In **event synchronous mode**, passcodes are generated when the button on the token is pressed. In **time synchronous mode**, passcodes are generated based on the clock rate set for the token. Choose one of the following:

- Event
- Time

2 Passcode length (applies to Alpine only)

Passcodes can be from four (4) digits to eight (8) digits in length. Choose one of the following:

- 4 digit
- 5 digit
- 6 digit (recommended)
- 7 digit
- 8 digit

3 Clock Rate (time synchronous mode only)

The passcode generation rate. Choose one of the following:

- 10 seconds
- 20 seconds
- 30 seconds (recommended)
- 60 seconds

4 SoftPIN

Associates a four-digit PIN to a token. This SoftPIN must be entered along with the token-generated passcode each time users authenticate with their token. Choose one of the following:

- Off (default)
- On

Using Alpine tokens

Alpine tokens were designed to be easy to use. When the user is prompted to authenticate to a SafeWord-protected resource, they only have to press the button on the Alpine token's face. The number displayed is the dynamic, one-time passcode the user will enter into the password field of the SafeWord challenge prompt.

If a SoftPIN option was chosen when the token was assigned, the user will also need to append or prepend that SoftPIN to the token-generated passcode when entering it into the password field.

Using other SafeWord-supported tokens

This section provides information about using the tokens. Be sure to pass appropriate information along to your users.

SafeWord Gold tokens

The SafeWord Gold includes a new user-friendly interface, and options that allow administrators and users to easily adapt the tokens to their specific security plan.

Figure 7: SafeWord Gold token



Table 1 gives a complete listing of SafeWord Gold token buttons and their functions, and Table 2 lists possible display prompts and their meanings.

Table 1: SafeWord Gold token buttons and functions

Button	Function
ON	Turns the token on or off
Clr	Clears the display of all information
<<	Deletes the last entered character
Ent	Generates a passcode
1 to 0 buttons	Used to input a PIN, host number, and challenge

Table 2: SafeWord Gold possible display prompts and meanings

Possible display prompt	Meaning
ERASEd	Token memory has been erased.
ENTR PIN	Enter your PIN.
NEW PIN	(Optional) Change the PIN after first use, or at predetermined intervals.
AGAIN	Retype PIN to verify.
SUCCESS	Displays after successful completion of a task.
NO MATCH	Displays after a failed PIN verification.
CHALLNG?	Enter SafeWord's challenge for passcode (used in DES x9.9).
HOST?	Prompts for host number (if token is programmed for multiple hosts).
bAd PIN	Displays if a bad PIN has been entered.
INVALid	Invalid host number was entered.
SAME PIN	Flashes if the same PIN was entered when a new PIN was required. User must change PIN.

SafeWord Gold initial operating modes

You determine the mode of SafeWord Gold tokens by the following:

- **Programmed mode**—When turned on, **ENTR PIN**, **passcode** or **CHALLNG?** appears.
- **Unprogrammed mode**—When turned on, **0** or **Erased** appears.

SafeWord Gold token options

SafeWord Gold token options include settings that allow only one passcode to display per use, and settings that force a user to change their PIN after the first use or after a specified number of uses. When the forced PIN change feature is enabled, the specified number of uses refers to the number of times that the PIN has been successfully entered for authentication. It is not related to the number of passcodes that have been generated.

SafeNet eToken 3300 (Platinum) tokens

The eToken 3300 includes a new user-friendly interface, and new options that allow both administrators and users to easily adapt the tokens to their specific security plan.

Figure 8: SafeNet eToken 3300 (Platinum) token



Table 3 lists buttons and functions, and Table 4 gives display prompt meanings.

Table 3: SafeNet 3300 token buttons and functions

Button	Function
ON	Turns the token on or off
Clr	Clears the display of all information
<<	Deletes the last entered character
Entr	Generates a passcode
1 to 0 buttons	Used to input a PIN, host number, and challenge
Pin	Allows user to input or change the PIN

Table 4: SafeNet 3300 possible display prompts and meanings

Possible display prompt	Meaning
ERASEd	Token memory has been erased and needs reprogramming.
ENTR PIN	Enter your PIN.
NEW PIN	Enter new PIN (optional setting, forces user to change their PIN after the first use, or at predetermined intervals).
AGAIN	Displays after a new PIN has been entered. Retype the PIN to verify PIN change.
SUCCESS	Displays after successful completion of a task.
NO MATCH	Displays after a failed PIN verification.
CHALLNG?	Enters SafeWord's challenge into the token for passcode. (Used in DES x9.9)
HOST?	Prompts user to enter the host number for which they need a passcode (if token is programmed for multiple hosts).
bAd PIN	Displays when a bad PIN has been entered.
INVALid	Displays if a bad host number is entered, or if the wrong number is entered during programming.
SAME PIN	Displays if the same PIN was entered when a new PIN is required. User must change their PIN.

SafeNet 3300 initial operating modes

Modes of SafeNet 3300 tokens are determined by the following:

- **Programmed mode**—When turned on, **ENTR PIN, passcode or CHALLNG?** appears.
- **Unprogrammed mode**—When turned on, **0** or **Erased** appears.

SafeNet 3300 token options

SafeNet 3300 token options include settings that allow only one passcode to display per use, forcing a user to change their PIN after the first use, or after a specified number of uses. When the forced PIN change feature is enabled, the specified number of uses refers to the number of times that the PIN has been successfully entered for authentication. It is not related to the number of passcodes that have been generated.

Programming the SafeNet 3300 token



Important: Before programming SafeNet 3300 tokens, refer to the CP Software User Guide that is included on the Card Programmer CD.

SafeNet 3300 tokens can be programmed using the CP software and the optional programming pen to transfer programming directly into the token. Token programming pens are available for purchase separately. For more information about ordering the Card Programmer token programming pen, contact your SafeNet sales representative.

Programming tokens

SafeWord tokens can be programmed using the Token Programmer Kit (TPK) software (for Alpine tokens), or the eToken OTP Programmer software.

Programming Alpine tokens using Token Programmer Kit software

The TPK software is a Windows-based application that allows you to specify programming options for your Alpine tokens. Using TP, you can specify unique configurations that are transferred into the token via the programming pen.

You can create a variety of custom TP configuration (*.tpc*) files that can be used as a “template” to program other tokens with the same settings. TPK software also generates files that provide information for the SafeWord database (*importalpine.dat*) and for administration purposes (*alpineuser.dat*). These files contain a record for each token you program.

TP kit software runs under the following Windows OS versions:

- Windows 2000
- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008

TPK software allows you to program SafeWord Alpine tokens with industry standard encryption algorithms that encrypt the on-board keys the tokens use to generate their displayed passcodes.

For specific information on using Token Programmer, see the *Token Programmer Kit User Guide*.

Programming tokens using eToken Programmer software

SafeWord Gold 7.0, SafeNet 3300, and eToken PASS event-sync/time-sync tokens may be programmed using the eToken OTP Programmer software. For more information about the eToken Programmer refer to the *eToken Programmer User Guide*.

Assigning SoftPINs to tokens

SoftPINs are four-digit personal identification numbers that can be associated with tokens. If a SoftPIN, has been assigned to a token, the user will need to know that PIN in order to authenticate with the token. They must enter the SoftPIN along with the token-generated passcode each time they authenticate. Generally SoftPINs are given to the users when they receive their tokens.

Deploying SafeWord-supported authenticators

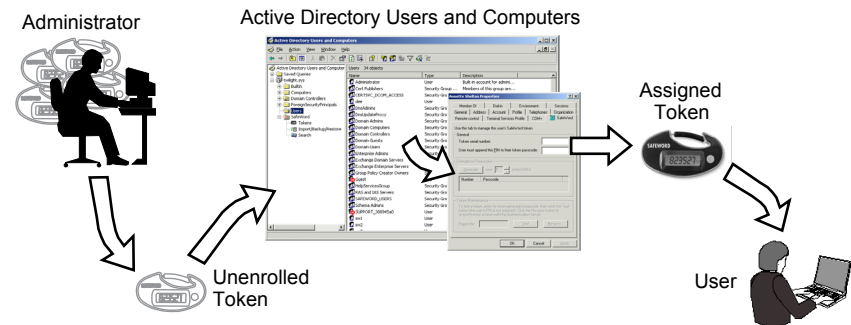
Before you can deploy your tokens, you need to import the token data files that were either downloaded during activation, or downloaded from the CD that came with your token pack. These token data files contain the individual serial numbers and programming information for your tokens, and allow the token to be “known” to SafeWord, and associated with a user in the user database.

Once the token data files have been imported, you can associate tokens to users as follows:

- 1 Select a token.
- 2 In ADUC, display the Properties window for a user.
- 3 Associate a token to that user by entering its serial number.
- 4 Give the (now) assigned token to the user.

Figure 9 shows this basic process.

Figure 9: Token deployment processes



Important: A token that displays '00000000' when you turn it on indicates an initialization mode. Do not store tokens in this initialized state. The '00000000' state is used only for programming tokens, and leaving them in this state causes premature battery drainage that will void all warranties. SafeNet ships all tokens, except the Alpine token, in a non-initialization state.

For support issues, contact SafeNet Technical Support at www.aladdin.com/support/safeword/default.aspx.

INDEX

A

- Alpine tokens 4, 5, 10, 11
 - clock rate 10
 - display mode 10
 - passcode length 10
 - programming options 10
 - SoftPINs 11
- asynchronous authentication 2, 3
- authentication
 - asynchronous 2, 3
 - challenge-response 2
 - event synchronous 2
 - synchronous 2
 - time synchronous 2
- Authentication Engine 3

C

- challenge-response 2, 3
- clock rate 10
- compliance
 - OATH 5

D

- display mode
 - event synchronous 10
 - time synchronous 10

E

- eToken PASS 8
 - using 8
- event synchronous 2, 5

F

- fixed passwords 6

- forced PIN change feature 13, 16

G

- Gold tokens
 - initial operating mode 13

H

- hardware tokens 4

M

- memorized passwords 6
- mode
 - one-time passcode 4
 - set a fixed number of PIN uses 4

O

- OATH compliance 5
- operating modes
 - SafeWord Gold tokens 13

P

- passcode length 10
- passcodes 5
- PIN change, forced 13, 16
- PIN mode
 - pre-expired 4
- PINs
 - resetting 9
- programming 13
- programming tokens 17

S

- SafeNet eToken 3300 (Platinum) tokens 14
- SafeWord Gold tokens 4
 - determining initial operating mode 13
 - using 12
- SoftPINs 11, 18
- synchronous authentication 2

T

- time synchronous 2
- time-synchronous 5
- Token Programmer Kit software 17
- tokens
 - Alpine 4, 5, 10
 - batteries 5
 - custom programming order form 10
 - customized 10
 - eToken PASS 4
 - hardware 4
 - initial operating modes for SafeNet 3300 16
 - options for SafeNet 3300 16
 - other vendors 4
 - programming SafeNet 3300 16
 - SafeNet eToken 3300 (Platinum) 4, 6
 - SafeWord Gold 4
 - SafeWord Gold operating modes 13
 - SafeWord Gold options 13
- TPK 17

W

- warranty 6



www.safenet-inc.com
4690 Millennium Drive, Belcamp, Maryland 21017 USA
Telephone: +1 410 931 7500 or 1 800 533 3958

©2011 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners.