

# One-time Password Tokens

CRYPTOCard Tokens are an effective and economical solution for organizations that want to eliminate the risks presented by static, shared, stolen or easily guessed passwords. With two-factor authentication, protected resources can only be accessed when a user combines their security Personal Identification Number (PIN), something only they know, with a one-time password generated by their unique authenticator for each logon.



## TOKEN TYPES:

### Key Chain Hardware Token (KT-1)

The KT-1 Key Chain token provides unparalleled convenience in a portable, independent computing environment. It's simplicity makes it the ideal authentication token for users of virtually any skill level.

The KT-1 Key Chain token generates a new password each time the token is activated.



### Calculator-style Hardware Token (RB-1)

The RB-1 PIN Pad token is a highly configurable, multi-function device and is the most versatile of the hardware tokens. It is ideally suited to users that require the freedom to logon from any computer, running any operating system, in any location, or generate digital signatures for web-based forms. It is also ideal for applications that require the use of challenge/response mode.

The RB-1 Key PIN Pad Token generates a new password each time the token is activated. The token is activated by entering a PIN using the keypad.



### End Users:

- Only need a PIN and a token
- Never need password changes
- Eliminate the use of static passwords

### Security Administrators:

- Control access of users
- Configurable tokens add security
- Web-based deployment of ST Tokens

### Budgets:

- Tokens never expire
- Reduced Help-Desk calls
- One-time licensing fees

### Flexibility:

- Wide range of tokens depending on what an organization requires

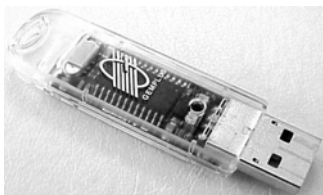
**Smart Card Token (SC-1) (with USB or PCMCIA Reader)**

The SC-1 Smart Card Token is a software implementation of the RB-1 hardware token installed on a 64K Java smart card. It is the ideal multi-function token card for organizations that want the advantages of hardware tokens, the convenience and integration of software tokens and the additional security of photo ID and proximity door access.



**USB Hardware/Smart Card Token (SC-3)**

The SC-3 USB token is a software implementation of the RB-1 hardware token installed on a USB packaged smart card. Ideal for organizations that want the advantages and flexibility of hardware tokens with the convenience and integration of software tokens. The SC-3 can also store digital certificates for PKI applications.



**Software Token for PC, WinCE or BlackBerry**

The ST-1 Token is a software implementation of the RB-1 hardware token for installation on computers and PDAs. It is the ideal token for organizations that want the strength of two-factor authentication without the overhead and cost of hardware distribution. For PC implementations, CRYPTOCard's M2M functionality provides an interface between the token and various authentication mechanisms, providing "One-PIN-And-You're-In" service.

ST-1 tokens can be installed on a PC hard drive, on a USB mass storage device, on a BlackBerry, or on a WinCE PDA.



**CRYPTOCard North America**

340 March Road  
Suite 600  
Ottawa, Ontario  
K2K 2E4 Canada

Toll Free: 800-307-7042  
Tel: +1-613-599-2441  
Fax: +1-613-599-2442  
E-mail: info@cryptocard.com

[www.cryptocard.com](http://www.cryptocard.com)

**CRYPTOCard Europe**

Eden Park, Ham Green  
Bristol BS20 0EB,  
United Kingdom

Tel: +44 870 7077 700  
Fax: +44 870 7077 711  
E-mail: info@cryptocard.com

[www.cryptocard.co.uk](http://www.cryptocard.co.uk)

CRYPTOCard and CRYPTO-Server are registered trademarks or trademarks of CRYPTOCard Inc. in Canada, the U.S.A. and/or other countries. Microsoft and Windows are registered trademarks or trademarks of Microsoft Corporation in the U.S. and/or other countries. All other trademarks mentioned herein are the property of their respective owners. © 2006 CRYPTOCard Inc. All rights reserved.

20070626