

## Protect Your Company's Most Valuable Asset!

### Information Theft – it's only the beginning...

In today's information age, your company's information is its most valuable asset. Your Hard Drive has become the intellectual property and a very important revenue stream of your business. But no longer is it safe...Laptops, PC's and Hard Drives are easily stolen and lost.

Information theft and espionage is on the increase. If large Banking Corporations are vulnerable to hacking and information theft, what about your information?



### Information Integrity

Your company carries privileged client and personnel information. At the very least, this information should be kept secured.

### The Repercussions...

What repercussions could occur, should your information be compromised? Your company could lose revenue, damage client-business relationships and be held legally accountable.

**SD Key** provides the solution in the form of **SD Key Data Encryption**, a local data security application. This innovative product integrates the latest in cryptography and USB technology for the Microsoft® platform.

This easy to use device will instantly secure (encrypt) your information (data) and e-mail. Securing your information will ultimately protect your revenue stream and prevent unauthorized access to that information. Even hardware theft will not pose a threat, as your information will remain inaccessible.



**SD Key Data Encryption** provides one thorough solution that offers the following features:

- Secure method of securing files and back-up files.
- Tamper-proof solution.
- Quick and safe file recovery system on lost or stolen Keys.
- User-friendly and easy to use.

**The SD Key Package Consists of:**

- (i) A robust USB Token
- (ii) a 128 KB Solid Encryption Process
- (iii) and a User On-line account



**The USB Token**

- Securely authenticates the user to their data.
- Each Key stores a unique, encrypted serial number. Trying to compromise secured data will require the intruder to compromise each Key independently.
- Designed to be robust and tamper-proof. Physical attempts to access the encapsulated chip will destroy it.
- Functions on the USB Platform. USB offers a much more secure method of connecting devices to machines.
- Losing Keys is not an issue because of the easy replacement method.
- Carried by the user as a key ring.

**The Software (Encryption) Program**

- This program encrypts all file types.
- Uses a solid encryption process to secure all sensitive and private information.
- Secures your e-mail by simply locking it with SD Key. This will firstly, secure the receiving end of e-mail and its attachments and secondly, prevent unauthorised access to that e-mail.
- Data that is encrypted will remain inaccessible from hackers.
- Using SD Key, hardware theft does not pose a threat, as your information will remain unattainable.
- Backup data can be stored in the encrypted format on removable storage device devices such as cd's or memory sticks. The data recovery process on lost or stolen Keys remains functional long after a particular Key has been replaced. This means the data stored thereon will not become redundant.
- Uses a "Secure Delete" function that securely deletes the original state (un-encrypted version thereof) of the file. With only the encrypted state thereof remaining.
- User-friendly - The user plugs in their Key to resume work and unplugs to secure the information.

## The User's On-line Account

- General support for the user including a Data Recovery Process, FAQ's and Help Libraries.
- Safe and easy Data Recovery Process - Whether locally or remotely based, the single user simply connects to the SD Key Website to instantly download the de-encryption patch for that specific lost Key or the organizational user contacts their IT Administrator.
- Lost and stolen Keys, once reported, are immediately "blacklisted". Once replaced these Keys will not function on the SD Key system and will not be able to unlock the data of its replaced Key.
- Program updates and add-ons will be available, to download, from the SD Key website.

## SD Key Token Range

SD Key (Pty) Ltd offers a range of Tokens to meet your specific level of security needs.

The Token Range Includes:

### 1. **Data Encryption Key**



Functions without a password and is recommended for the user with standard security priorities. Passwords are generally not advised for the user with standard security priorities – refer to the Password Discussion below for the reasoning.

### 2. **Plus Token**



Colour subject to change

Securely stores a password and therefore caters for the users that require a higher level of security needs.

---

Directors:  
A Herzberg, W.F. van Zyl, J.H Gouws

**PROUDLY**  
**SOUTH AFRICAN**   
Copyright SD Key (Pty) Ltd

## **The Password-only Solution vs. SD Key Data Encryption Solution**

Data Security applications that only uses a password only offers a first level of security to protect data. The program may be relatively good but the weakness lies in the use of a password, as will be discussed below. In summary the password offers no back up support on lost, compromised or forgotten passwords.

The SD Key Data Encryption Program offers a robust system using a solid encryption process to encrypt data with. The physical token is carried by the user (similar to a car key), and is virtually tamperproof. This solution offers a safe data recovery process on lost or stolen Keys.

**Problem 1.** Passwords only hinder a potential intruder. With enough time, technical know-how and calculated guessing, the potential hacker can easily hack into your private files that are only password protected, simply because there is no second level of authentication such as the SD Key token, a physical device.

**Solution** It is nearly impossible for a potential intruder to hack into data that has been encrypted with the SD Key solution. The SD Key is a physical device that has to be present for de-encryption.

**Problem 2.** Passwords that cannot be remembered or found for a particular document can be disastrous when you are trying to access it.

**Solution** SD Key offers a safe and easy data recovery process on lost or stolen Keys that remains functional long after that particular Key is replaced.

**Problem 3.** Passwords do not have a time delay or a cut out facility. Should a potential hacker hack into your data they can do it at their leisure.

**Solution** SD Key has a time-delay feature that hinders tampering on the chipset.

**Problem 4.** Passwords are entered via the keyboard. There is Spy software available that is able to capture the entries made on the keyboard and mouse functions.

**Solution** The SD Key program reads the encrypted serial number. The original serial number is un-obtainable and the encrypted serial number is useless.

**Problem 5.** Passwords need to be typed in for each document that you want to open and every time the document is opened. It is therefore time-consuming.

**Solution** Simply plug in your SD Key to resume work.

**Problem 6.** Passwords are quite general and a lot if programs require them. How many individual passwords do you use and are able to remember?

**Solution** You can use SD Key to secure many data files.

**Problem 7.** Passwords that are effective are lengthy and intricate  
e.g. eoui4745jfsqt42809mgjk.

**Solution** Who can remember that? The encrypted serial number makes for an effective password. There is nothing to write down. Simply take care of your Key.

Problem 8. Passwords are usually written down for the above-mentioned reason, but writing it down means that it is vulnerable of being found.

Solution Once again, the encrypted serial number makes for an effective password. The original serial number is un-obtainable. Simply take care of your Key.

Problem 9. Users are negligent with password as they forget, misplace and share them. The user has therefore no support should their password be compromised. The password is therefore only as effective as the user handles them.

Solution With the SD Key Solution, the user merely has to take care of their token. The user has support on lost or stolen Keys and immediate action will prevent your data from being compromised.

Problem 10. Users are often required to change passwords regularly in the interest of security. Changing passwords often means that users will forget them more often.

Solution The only time a Key is changed is when it is reported lost or stolen.

Problem 11. Users usually use their personal information as a password e.g. a birth date. What do you use?

Solution The encrypted serial number makes for an effective password. The original serial number is un-obtainable. Simply take care of your Key.

### **In Summary**

The limitations of passwords are obvious and it should therefore not be used as a primary security method, but rather as an additional level of security.

### **Company Introduction**

**SD Key (Pty) Ltd** is a software development company specializing in information security.

### **"Proudly South African" Member**

SD Key is designed and produced locally; hence SD Key (Pty) Ltd is proud to be a "Proudly South African" member.