TrustedSignins™ from SanDisk®

Easy to Buy, Easy to Use

For many years, an account name and unchanging (or infrequently changing) password have been used to gain telephone or online access to an individual's bank, brokerage, or other accounts. But account names aren't necessarily private and passwords can be stolen, guessed, or even shared. In fact, with the dozens of account names and passwords that people need to remember, many of them get written down.

This has been considered an acceptable risk—until now—when many governments are mandating the use of tokens that generate a one-time password for financial transactions and companies and gaming sites are now encouraging their use as well. Unfortunately, your customers and employees soon may find themselves with a necklace of tokens—one for each site or account—that except for granting access can't do anything else. And that leads to dissatisfaction. TrustedSignins supports multiple virtual tokens that can be used to authenticate to hundreds of institutions.

Partnering With the Best

Partnering with RSA Security and VeriSign, the security industry's biggest names, SanDisk, the world's leading supplier of flash memory data storage card products, has developed TrustedSignins. This revolutionary solution runs on a standard SanDisk USB flash memory device (UFD) and TrustedFlash™ memory cards for mobile devices such as phones and handheld game consoles.

A benefit of TrustedSignins over dedicated tokens is that your company does not need to bear the expense of stocking and supplying them to your customers. After an employee or customer buys a standard SanDisk device at any of the 185,000 retail locations, it is registered with their account at your company. As an incentive, your company can even offer a rebate.

SanDisk®

TrustedFlash Technology
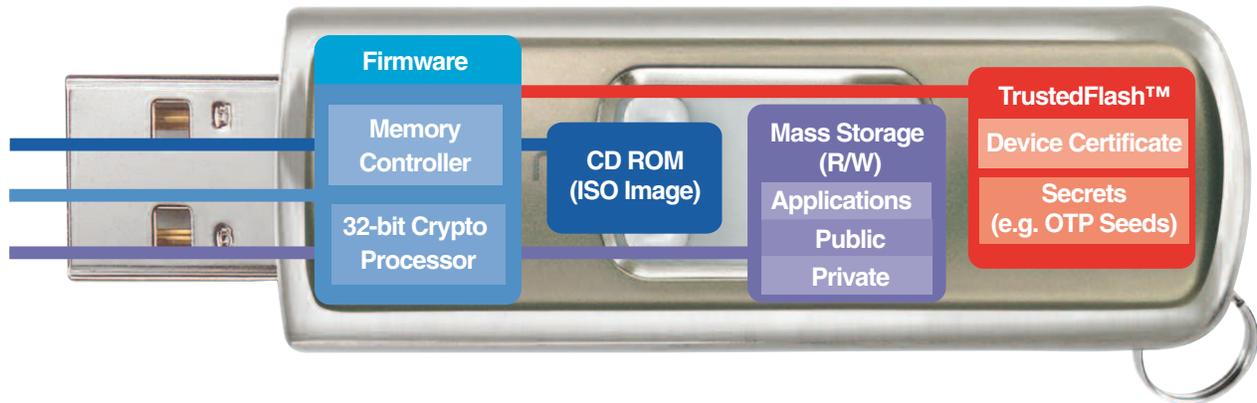
TrustedSignins is based on SanDisk's TrustedFlash technology. Every TrustedFlash device contains a unique readable electronic serial number, a device certificate, and an unknown random encryption key. A custom controller partitions memory and manages access from the host PC. A 32-bit cryptographic co-processor automatically encrypts and decrypts all data written to and read from the device, protecting against information disclosure even if the components are directly targeted.

The host OS has no direct access to TrustedFlash memory. The device API supports strong authentication, including PKI, allowing authorized host processes to create and access their own information in the TrustedFlash partition while preventing access even by other processes authorized to access other information within the TrustedFlash partition. For example, the shared secret used to generate a one time password can be written and erased but not read from the device. Similarly, the device certificate can be used for authentication, verification, and signing but cannot be modified. The device certificate can be encapsulated in a PKCS#7 package, thus supporting PKI applications.

SanDisk USB flash drives can make 3 disk volumes available to the host PC; a read-only CD ROM image, a public volume, and a password-protected private volume.*

For more information on TrustedFlash technology or TrustedSignins and how they can increase security while lowering costs, please send an email to **Trustedsignins@sandisk.com**

Features and Advantages
- Based on TrustedFlash™ Secure Storage Technology
- One device supports multiple virtual tokens and multiple algorithms
- OATH (Open Authentication) compliant
- Up to 4.0GB of password protected flash memory storage

* TrustedSignins and the private volume require Windows 2000 Service Pack 4 and later, Windows XP (all editions and service packs), and Windows Server 2003.