DESIGNING SECURE USB-BASED DONGLES

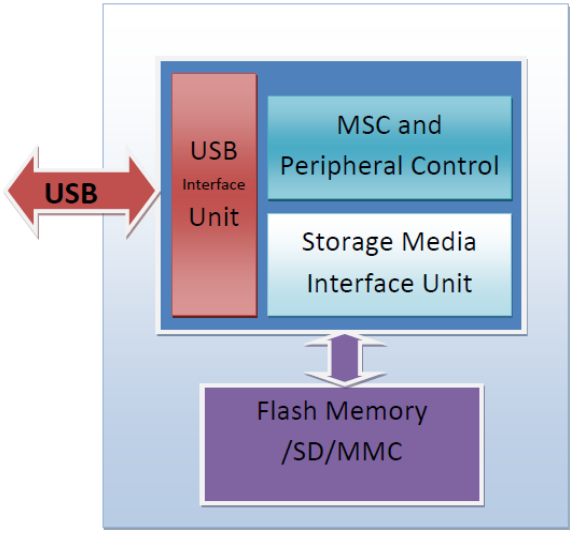
By Dhanraj Rajput, Applications Engineer Senior, Cypress Semiconductor Corp.

The many advantages of USB Flash drives have led to their widespread use for data storage through every industry. However, given that these drives are highly portable, care must be taken to protect private and sensitive data from theft and accidental loss of the drives.

USB Flash drives which implement security features are generally called USB Secure Dongles or Secure Dongles. There are various ways to design a secure dongle and the best secure dongle for a specific application balances system cost with the level of security required for a particular application. This article will describe techniques for designing secure dongles.

USB Flash Drive Architecture

A USB Flash drive consists of two main components (see Figure 1): a USB mass storage controller and non-volatile memory (storage media). Most USB Flash drives employ a two-chip architecture. The USB mass storage controller integrates USB functionality with the transceiver, storage controller, and optional interfaces for LEDs, switches, etc. The storage media is used to store user data, like files and folders. NAND Flash or Managed NANDs are most commonly used as storage media.



The USB mass storage controller acts as a bridge between the storage media and USB host. It perform various tasks which can be roughly divided into three functions:

1. USB Mass Storage Class (MSC) Management
2. Storage Media Management
3. Peripheral Control (optional)

The USB Flash Drive uses the USB Mass Storage Class over two bulk end-points to communicate with the Host. The USB mass storage controller is responsible for USB enumeration and MSC handling.

If SLC/MLC NAND is used as the storage media, then storage media management involves wear leveling, bad block tracking, Error Correcting Code (ECC) protection, and NAND interface handling. If managed NAND is used as the storage media, then wear leveling, bad block and ECC are managed by the NAND itself. In a generic USB Flash Drive, access to memory is transparent to the USB controller and host and there is no control over it.

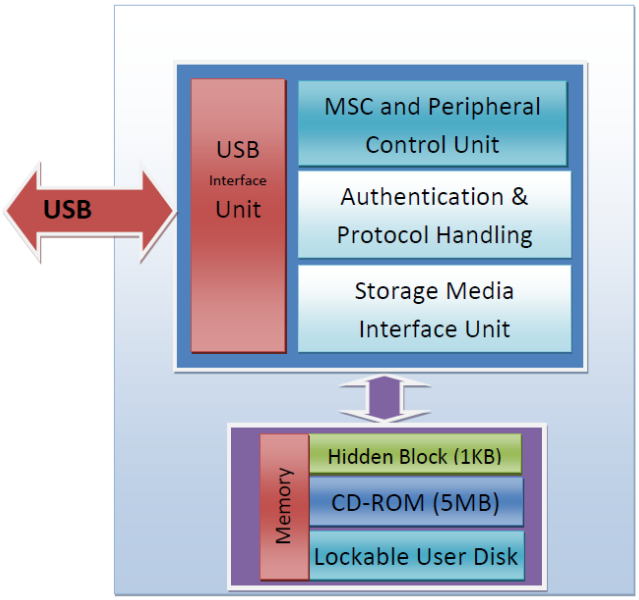
Published in EE Times Industrial Control (http://wwweetimes.com) December 2011

Secure Dongle for Personal Storage

USB flash drives are widely used for carrying personal data can be protected by simple security such as a password. Software is available on the Internet for more advanced forms of data protection. This software can be used with any generic USB Flash drive to make it password protected but there are security vulnerabilities to such an approach:

- The data or security software on the drive can be easily erased by reformatting it.
- Special software needs to be preinstalled on the PC to access the data. To access the drive from a new system, this software must first be downloaded from the Internet and installed, thereby limiting the convenience of using a Flash drive.

An alternative approach is for the Flash drive to carry any security software required to access data in a separate partition which cannot be erased. This can be done without any additional hardware provided the USB Mass storage controller has the flexibility to be able to partition memory and then control access to each memory partition. Controllers on the market today, such as Cypress's West Bridge Astoria and NX2LP, are available which have features like these.



As per the USB MSC spec, a Flash drive can have as many as sixteen logical units (LUNs). These appear as separate drives to the USB host. The logical unit can be removable, read only (ROM) or read/write enabled. As shown in Figure 2, the storage media needs to be divided into three LUNs for a protected scheme:

- One ROM LUN as big as necessary to store the secure application
- One or more read/write LUNs for user data
- One hidden block, accessible only to the USB Mass Storage Controller firmware, to store passwords, disk status, and other identification data.

The secure application uses a SCSI Pass-Through mechanism to communicate with the Flash drive to lock the user LUN, unlock the user LUN, erase the user LUN, and set the password.

The MSC allows SCSI Pass-through (SPT) commands from the USB host. The SPT mechanism can also be used to handle non-mass storage activities from the host like setting the password, locking the dongle, and verifying the password for unlocking the Dongle.

Below is a step-by-step description of secure dongle behavior when connected to a Windows PC.

Device Enumeration:

When connected to a Windows PC, the Flash drive enumerates as a standard mass storage device. Two additional disks appear in Windows Explorer:*

- A CD-ROM disk of around 5MB size that contains the secure application
- A user disk in locked state that prevents the disk from being opened

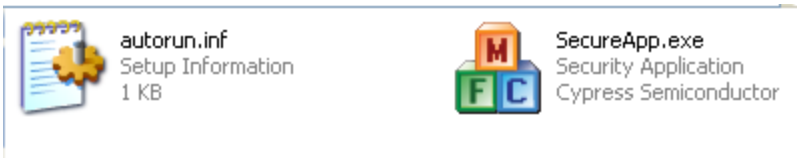
The size of the user disk is the size of the storage media being used minus the size of the secure application partition. At this stage, all read and write operations to this disk from USB host are blocked by the firmware. If a user tries to access the disk via a Windows PC, it will pop up the notification, “Please insert the disk”.

** If the Flash drive is connected for first time to the Windows PC, the standard procedure for installing the mass storage drivers needs to be followed.*

Auto Run : Secure App:

Device enumeration as described above is a quick process that is transparent to the user. When the device is connected to the PC, the user sees the “SecureApp” Window first (see Figure 3). This Demonstration Application (SeureApp) use SPT commands to identify, unlock, lock, and erase the user disk.

This App is stored in the CD-ROM partition of the dongle along with the “autorun.inf” file (see Figure 4).



The autorun.inf file contains following two lines which run the SecureApp automatically when the dongle is connected.

[autorun]

OPEN=SecureApp.exe

Device Identification:

When the SecureAppis starts, it checks the status of the device by sending a status SPT command. When the device receives a status command, it determines whether it is communicating to the correct device. It also retrieves the configuration of the device such as whether password is set or not. If the password has not been set before for the device, then any user partitions are accessible for read/write without any authentication, and SecureApp asks the user to set the password (see Figure 5).

User Authentication:

If a password has already been set for the device, then the user is asked to provide the password to unlock the user disk. The user password is stored inside the storage media in a secure sector that can only be accessed by device firmware. Typing the password and clicking on unlock sends the password to the device using SPT. This password can be encrypted if desired. The device verifies the password internally and unlocks the media if the password is correct. File read/write operations are now allowed to the disk.

Erase Password:

If the user forgets the password, the data stored on the drive will be completely inaccessible. However, the dongle can still be used by using the Erase password feature to first delete all user data and then allow the user to set a new password.

Advantages of this architecture:

- Low cost: no special hardware is required.
- Standard Mass storage driver: no special driver/software need to be installed on PC.
- Higher throughput: data transfers between the PC and dongle are uninterrupted since there no encryption is used to transfer data. This results, for example, in less time to transfer large video files.

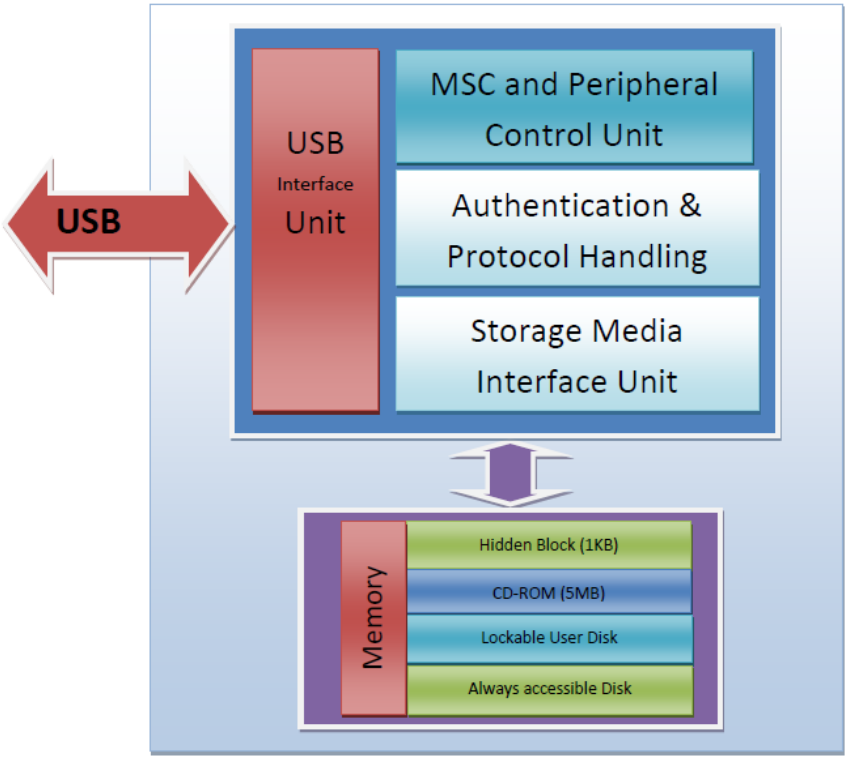
Secure Dongles for Medical Applications

USB Flash drives are now being used to store medical information like:

1. Emergency data
2. Health records

3. Lifestyle information
4. Prescription information
5. Miscellaneous data like X-Rays and MRI files

Such a dongle contains public information that needs to be accessible to anyone, such as information that can be used in the case of an emergency. However, the dongle also contains private information that requires authentication to access. A dongle might also offer additional features like backup of data on a web server when connected to a PC with an Internet connection or formatted representation of data for printing or editing.



A secure dongle with storage memory partitioned into three can be used for such an application:

- CD-ROM Partition for storing the application
- Standard (unprotected) read/write partition for storing publically accessible data like Emergency data
- A protected partition which can only be accessed after user authentication

As shown in Figure 6, the hardware described in the section “secure dongle for personal storage” can be used here as-is. There is only change is in the way storage is managed to support the extra partition. Additionally, the application stored in the CD-ROM partition may need to offer additional functionality beyond the SecureApp such as an application to display health records in a printable format.

Secure Dongles for Banking

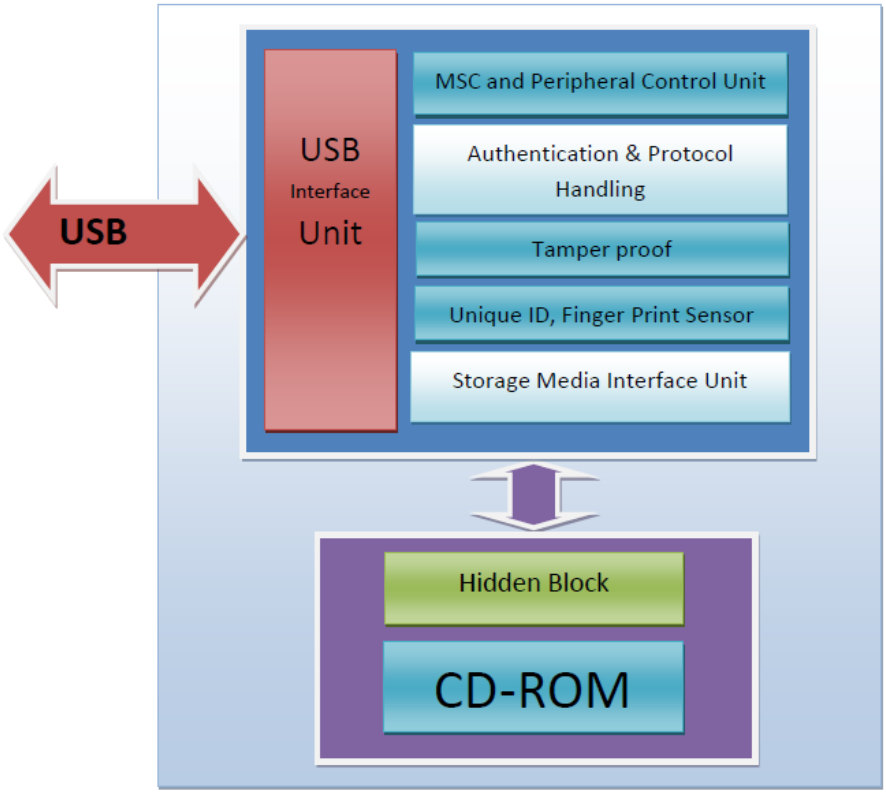
Well-known risks to Internet banking include key loggers, screen readers, root-kits, botnets, Trojan, spyware, malware, and phishing which compromise the user PC. One way to avoid these risks is to operate from a clean OS. Most of the latest PCs and laptops support boot from USB Flash drive where user can use the system without launching the OS on the system hard

drive. Such an OS boots quickly and can be read-only where any other application other than those built into the Flash drive cannot be installed or run. An example implementation for such an architecture is shown in Figure 7. It contains the following different units/features:

1. USB Mass Storage Class(MSC) Management
2. Storage Media Management
3. Finger Print sensor(optional)
4. Unique ID
5. Tamper Proof
6. Encryption unit.

USB Mass Storage Class (MSC) Management: For the PC/laptop to boot from the USB disk drive, the drive must comply with the USB Mass Storage class. The dongle should enumerate as Read-Only device. This protects the OS and the drive from any intended or unintended corruption.

Storage Media Management: The storage media used here can be NAND Flash or SD-MMC based Managed NAND. The media should be portioned into a read-only partition for storing the OS and another hidden partition for storing secure data like the server ID, user ID, finger print data, etc. Any write access to the read-only partition and read/write operations to hidden partition from the USB host should be blocked by the storage media management unit. The hidden partition is accessible internally to the device only. It is also a good idea to use encryption for storing secure data in the hidden partition.



Finger Print Sensor: Access to the banking server is handled by the dongle but before the dongle begins communicating to the Banking Server, it first authenticates the user. User authentication can be done in multiple ways e.g. providing a password (PIN), figure print info, etc. A finger print sensor is more secure than a password mechanism but it comes at extra cost. The password/finger print info provided by the user is verified by the dongle using the information stored in the hidden block.

Considering the level of security required for banking applications, these dongles should be tamper-proof and non-clonable. Device cloning can be avoided by implementing a unique ID in device hardware. Battery-powered mechanisms can be used to make the dongle tamper-proof. Such a mechanism should erase the entire dongle data if any unauthorized activity is detected.

Cypress Semiconductor
198 Champion Court
San Jose, CA 95134-1709
Phone: 408-943-2600
Fax: 408-943-4730
http://www.cypress.com