Encrypted USB Flash Disk

by Yingbo Hu,
R&D Embedded Software Engineer

This Tech Note describes a possible use of the smxUSBH host stack and smxUSBD device stack in the same system in order to encrypt a USB flash disk.

The target system could be considered to be a special USB "cable" that connects the USB flash disk to the host computer and does encryption/decryption of the data that passes through it.

First, a normal USB flash disk is plugged into the host port of the target, and smxUSBH retrieves all the flash disk information such as total size and sector size. Then the device port of the target is connected to another host, such as a Windows PC. smxUSBD will report to the PC that it is "virtual flash disk" with the same size as the real flash disk connected to the host port. When the Windows PC wants to read data from the "virtual flash disk", smxUSBD's mass storage function Read() is called, and this function calls smxUSBH's mass storage function su_MStorIO() to get the data from the real flash disk. The Read() function decrypts the data and returns it to the PC. To write data is the reverse procedure; it encrypts the data. The following diagram summarizes the process:

Read: flash disk raw data → smxUSBH → decrypt → smxUSBD → Host
Write: Host → smxUSBD → encrypt → smxUSBH → flash disk raw data

The end result is that the flash disk can only be seen by a PC if it is plugged into the "cable". Otherwise the data is unreadable.

Please contact me with any comments or questions about this article.

Yingbo Hu
R&D Embedded Software Engineer
Micro Digital Inc
1-800-366-2491