

OXUFx94x Series Highlights

- High performance, low power SATA storage controllers with integrated hardware encryption
- On-chip hardware cipher engine supporting:
 - 128-bit and 256-bit encryption keys
 - AES-ECB, AES-CBC and AES-XTS algorithms
- Host software and driver supplied for password application for PC and Mac
- Support for up to 2 SATA II compliant ports (OXUFS946DSE)
 - With SATA Interface Power Management (IPM)
- Capable of supporting burst data transfer rates at up to 300MByte/s with sustained transfer rates in excess of 250MByte/s
- Market proven 1394b PHY interface and Link Layer with industry leading performance



Application:

Direct Attached Storage (DAS) – Secure Personal Storage Solutions

PLX Product:

OXUFx94x Series SATA Controllers

Key Benefit:

Protecting and defending stored personal data is simplicity itself

Issues of information security, identity theft and privacy are concerns for everyone, not just businesses and those involved in national security. Anyone who stores personal or sensitive data such as financial data, transaction records, banking details and password files, not to mention digital photos or video clips, should take steps to defend the data from accidental loss and malicious theft.

But in reality very few people actually do, since the generally held assumption is that the risks are largely associated with the internet and the transmission of data. The fact is that as a result of the highly portable nature of today's storage devices, it is just as likely that the data loss happens because of physical loss or theft of the storage device from work, home or while in transit.

A series of high-profile examples has recently brought home this point. Last year 76 million US veterans' records were placed at risk when a National Archives and Records Administration contractor improperly disposed of a hard drive containing health records and discharge papers. In 2008 the mobile network operator, T-Mobile, reported the loss of a hard disk containing data on more than 17 million customers. In the same year a hard drive was purchased off eBay that contained personal and account details of around 1 million Royal Bank of Scotland customers. Most recently the Arkansas National Guard reported that an unencrypted external backup drive holding the names, social security numbers and other unspecified personal information of more than 35,000 guardsmen was missing. And in a recent study, the Ponemon Institute claims that in the past year, more than 800,000 data-sensitive memory devices were lost or stolen.

Securing Data at Rest: Software vs Hardware

The impact of a data loss or theft incident can be neutralized if the data is encrypted on the storage media, commonly referred to as *securing data at rest*. The result is that if the storage system or media falls into the wrong hands, when the unauthorized user tries to access the data, only a string of random characters can be viewed rather than the actual data file.

Software-based data encryption systems, such as Windows BitLocker or TrueCrypt, have been around for some time but have failed to gain significant traction as they represent a serious drain on the host PC's processing power, thus resulting in sluggish performance and unresponsive systems. As a result, when using most software-based data encryption systems, typically only a sub-set of the data is encrypted to reduce the processing burden, and then the issue becomes one of determining what data needs to be encrypted and what doesn't.

Hardware encryption systems offer a simple way to address both the performance impact and data classification issues of software-based encryption systems. A hardware-based system automatically encrypts all data to be written to the media, and can be completely transparent to the host while operating at full disk rates.

OXUFx94x: A complete solution for Secure Consumer Storage

The PLX OXUFx94x series of SATA controllers bridge from USB 2.0, FireWire or eSATA to either 1 or 2 SATA ports.

Each controller integrates hardware encryption implementing the Advanced Encryption Standard (AES) and data written to the media, so only a user with the authorized key can access the data on the media. The embedded cipher engine supports the following NIST (National Institute of Standards and Technology) approved algorithms allowing them to be used in FIPS-140-compliant encryption products:

- AES-ECB (Electronic Code Book)
 - The simplest implementation of the AES algorithm.
 - The data is divided into blocks and each block is encrypted separately
- AES-CBC (Cipher-Block Chaining)
 - Uses an initialization vector and feeds forward encrypted data stronger cipher-text result than ECB
- AES-XTS (XEX-based Tweaked CodeBook with CipherText Stealing)
 - Algorithm developed specifically to address the needs of protecting data at rest, also known as IEEE 1619-2007
 - NIST recommended algorithm for Confidentiality on Block-Oriented Storage Devices i.e. direct attached hard disk drives

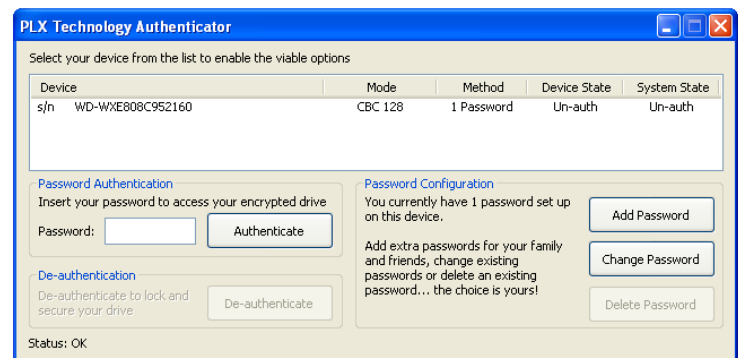
The design and implementation of a secure storage system involves a lot more than simply encrypting and decrypting the data. A fully functional system must also handle:

- Key management including the generation of all encryption keys as well as secure storage of necessary keys
- User verification to prevent access to the data by illegal users, referred to as user authentication and de-authentication.
- The mounting and safe ejecting of the media to the host system

In addition to the device and firmware required to implement encrypted storage systems, PLX also provide host software for Windows PC's and Mac's to perform all required key management, user authentication and mounting/removal of the encrypted drives on the host system.

The PLX Authenticator application provides an easily-customizable front-end for key management, user authentication as well as mounting the encrypted volumes on the host platform. The Authenticator supports:

- Generation of 128-bit or 256-bit data encryption keys
- Secure storage of encryption keys
- Creating, changing or deleting of users passwords. Up to 10 passwords can be defined
- User authentication and mounting of the drive
- Safe user de-authentication and ejecting of the drive



PLX Authenticator for Windows PCs

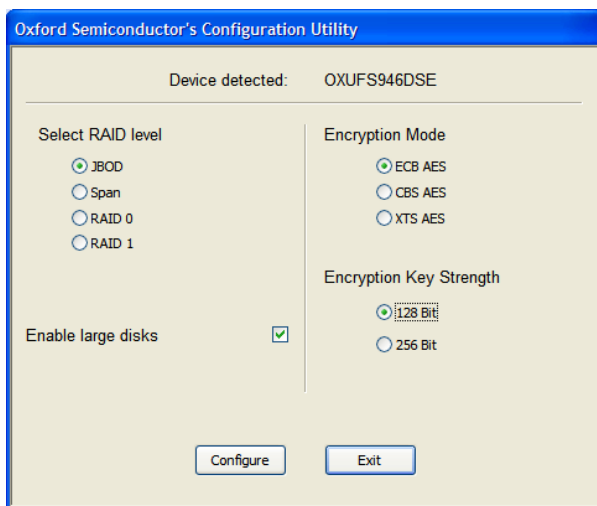


PLX Authenticator for MAC OS

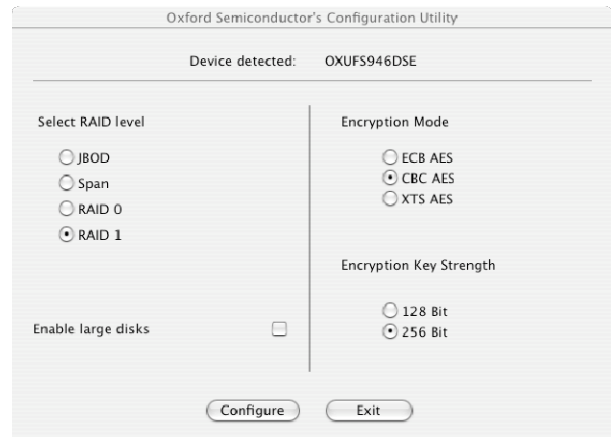
Optimized Firmware and Flexible User Agent

PLX DAS controllers are supplied with fully featured, optimized firmware tailored to the target application. The base firmware for the OXUFx94x controllers includes all standard features that are required to deploy a secure personal storage system for consumer applications, including a configuration utility.

The PLX Configurator utility is an easy to use, host application, for selecting the encryption algorithm and the key strength. In addition for multi-disk SATA controllers the Configurator can be used to define the current RAID mode. The PLX Configurator is supplied as a customizable framework which OEMs can tailor to meet their individual branding requirements.



PLX Configurator for Windows



PLX Configurator for MAC OS

Development Tools & Custom Solutions

PLX offers a comprehensive development and support package for the OXUFx94x series including:

Rapid Development Kit (RDK)

- Evaluation board with pre-built firmware application for product demo and evaluation
- Reference design schematics for reduced time-to-market
- Product documentation & application notes

Software Development Kit (SDK)

- Full source code to facilitate product differentiation and customization
- Debug hardware
- Compilers, drivers, programming utilities and complete documentation

Additional PLX Advantages

- Superior storage expertise
- Robust and market-proven storage system solutions with full feature set
- Schematic and Layout Design Reviews
- Regional support teams for fast time-to-market

Available on PLX Website:

Product Brief, Databook, Application Notes, technical support
<http://www.plxtech.com/products/consumer/#das>