

# Enabling Enterprise-Wide Data Security

The Virtex family of FPGAs provides a flexible hardware architecture for Decru's storage security solutions.

by Michele Borovac  
Director of Marketing,  
Decru — A NetApp Company  
[michele@decru.com](mailto:michele@decru.com)

Sriram R. Chelluri  
Senior Manager, Storage and Servers  
Xilinx, Inc.  
[sriram.chelluri@xilinx.com](mailto:sriram.chelluri@xilinx.com)

Many technology-based trade publications started off the year with a recap of critical personal data loss or theft incidents caused by criminals or sheer negligence. Some of the high-profile incidents that made the news included:

- U.S. Department of Justice — the loss of a laptop containing Social Security numbers and other personal data affecting 80,000 people
- LaSalle Bank/ABM Amro — a backup tape containing information about 2 million clients went missing. Although it was eventually located, ABN still had to notify its customers, as they could not verify that the data wasn't breached while the tape was missing
- Marriott — Social Security and credit card numbers as well as personal information about 206,000 customers and employees went missing
- Bank of America — Lost data tapes containing information on 1.2 million federal employees

# With Decru DataFort, enterprises and government organizations can fully leverage the benefits of networked storage, confident that their data assets are secure.

A recent survey by Network Computing magazine readers ranked “data security/privacy” as the number-one concern for IT administrators. When data goes missing, the problem is far greater than just losing data. The Federal Trade Commission estimates that at least 10 million people have had their identity stolen, resulting in an estimated \$5 billion in damages for individuals and \$48 billion for businesses. Both state and federal governments have stepped in with regulations designed to better protect consumer privacy and increase the penalties for companies that fail to protect this data.

2005 was the tipping point when corporate and government IT managers recognized the need to secure sensitive data at rest, before their company became front-page news. 2006 will prove to be the year that enterprises address this problem. Gartner, a major industry research group, predicts that “by year-end 2006, failure to encrypt credit card numbers stored in a database will be considered legal negligence in civil cases of unauthorized disclosures.”

Decru DataFort storage security appliances represent the first and only unified wire-speed encryption platform for securing stored data across the enterprise, with support for NAS, DAS, SAN, iSCSI, and tape backup environments. DataFort appliances are operationally transparent and do not require any software to be installed on clients, servers, or storage devices (Figure 1).

Key data security applications for the enterprise include:

- Secure storage consolidation
- Insider threat mitigation
- Regulatory compliance
- Database security
- Secure tape backup and disaster recovery

With Decru DataFort, enterprises and government organizations can fully leverage the benefits of networked storage, confident that their data assets are secure.

## Data Security Challenges

Traditional software-based encryption methods running on generic CPU architectures and specific OS environments are notoriously slow and cumbersome to implement. Strong encryption is computationally expensive and therefore consumes the most hardware resources, leaving little processing time for other tasks.

ASIC-based systems can be expensive, with long lead times, higher costs, and risk, and they are not upgradable. As encryption standards change, products can become obsolete, requiring customers to rip-and-replace to meet emerging security stan-

## Decru Storage Security Solutions

Decru DataFort storage security appliances leverage Xilinx® FPGA technology to enable high-performance encryption and compression, with the added flexibility to upgrade DataFort firmware to support new features and emerging standards. In addition to performance and easy implementation, another critical consideration for an encryption solution is the security of the system itself.

## Hardened Architecture

Software-based or application-level encryption solutions typically do not have a secure

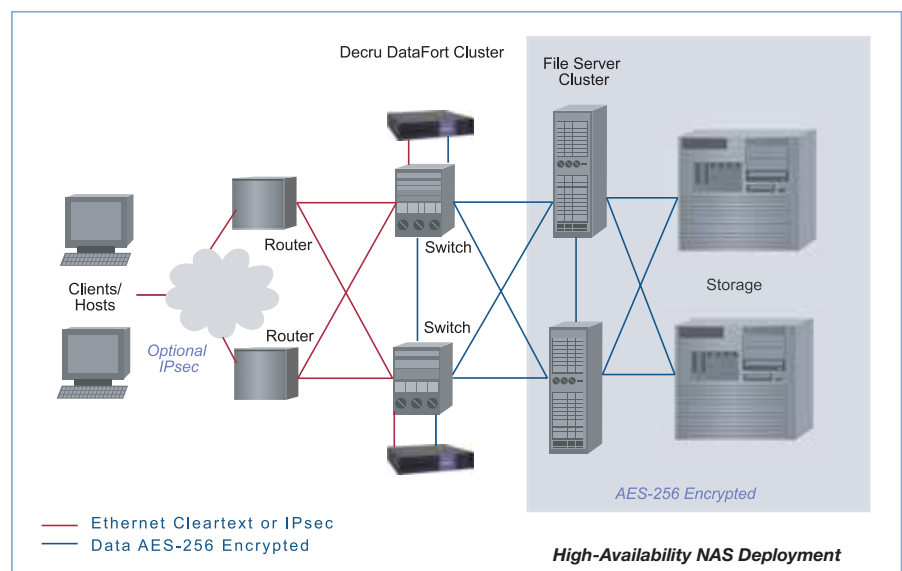


Figure 1 – High-availability deployment

dards. This leads to a solution that is not future-proof. As an example, Microsoft banned the use of DES, MD4, MD5, and in some cases the SHA-1 encryption algorithm, making 50% of some ASIC-based encryption functionality obsolete.

ASIC-based encryption solutions cannot easily adapt to incorporate new standards, forcing customers to continue purchasing hardware each time new encryption features are needed.

method for storing encryption keys: keys are kept in clear text in an open operating system. This is a recipe for disaster if someone gains access to that machine.

DataFort appliances are designed from the ground up to protect stored data, using security-optimized hardware that is less vulnerable to attack than off-the-shelf hardware and software solutions. At the heart of the appliance is the storage encryption processor (SEP), a hardware engine

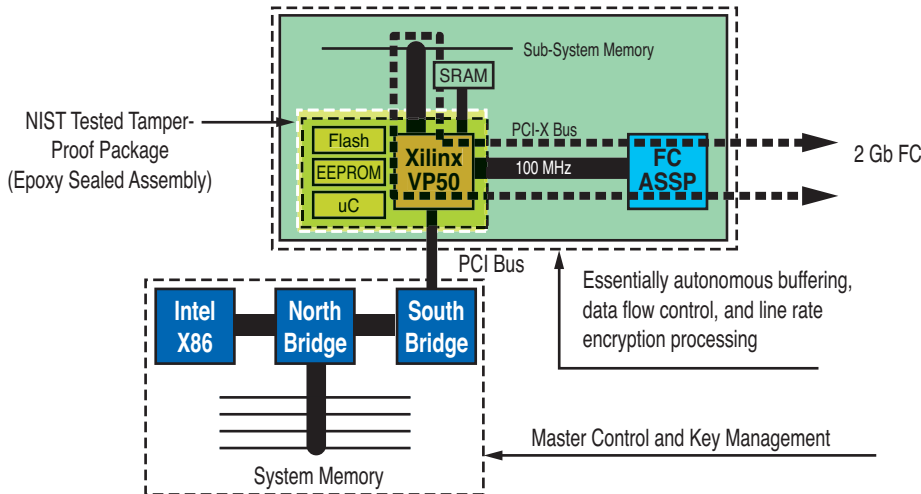


Figure 2 – Virtex-based encryption processing

that performs wire-speed, low-latency encryption and decryption while ensuring both data and key security.

DataFort appliances combine hardware-based AES-256 encryption, authentication, strong access controls, and crypto-signed logging in a hardened platform optimized for performance and reliability. DataFort appliances can be deployed in active/active clusters for availability and failover, and additional appliances can be added to address higher throughput requirements.

#### Application Coprocessing

To meet their design and time-to-market goals, Decru selected Xilinx Virtex™-II Pro FPGAs. An FPGA-based configurable coprocessing solution enables Decru DataFort appliances to:

- Adapt to changing encryption standards
- Add new features to systems already deployed at customer sites
- Meet performance and scalability requirements
- Support a broad range of features and performance at various price points
- Reconfigure hardware to adapt to customer requirements (Figure 2)

The Virtex product line comprises low-power and high-performance FPGAs capable of supporting 10 Gbps. Both Virtex-II Pro and Virtex-4 devices feature embedded PowerPC™ 405 hardware cores that run at

speeds as fast as 450 MHz, soft IP cores such as the 32-bit MicroBlaze™ RISC processor, and up to 200,000 cells of configurable logic. The Virtex-4 series features a scalable Advanced Silicon Modular Block (ASMBL) architecture that has allowed Xilinx to produce a programmable silicon platform with unprecedented capabilities and configurations to build coprocessing solutions.

In the Decru solution, the Virtex FPGAs enable wire-speed encryption and compression for tape appliances.

#### Conclusion

To defend against the increasing number of attacks on data at rest, IT managers are implementing data encryption technology solutions to protect sensitive or regulated data. An adaptable, special-purpose data security coprocessor is the foundation for Decru's FPGA-based encryption appliance.

Decru DataFort appliances, based on the Xilinx Virtex family, provide the only unified platform available to secure data at rest across the enterprise. DataFort appliances lock down sensitive data without degrading network performance or requiring costly changes to the storage environment. By using Xilinx FPGAs, Decru can provide a high-performance, highly scalable encryption solution.

For more information about Decru DataFort appliances, visit [www.decru.com](http://www.decru.com) or e-mail [info@decru.com](mailto:info@decru.com). To learn more about implementing reconfigurable computing solutions, contact [sriram.chelluri@xilinx.com](mailto:sriram.chelluri@xilinx.com).

Supporting Your Future  
**HUNT ENGINEERING**  
USB connected Programmable FPGA systems

### V-II Pro PowerPC

- Virtex-II Pro XC2VP7
- 256 Mbytes DDR Memory
- Configurable digital I/Os
- PowerPC boot FLASH
- USB 2 or Standalone

### Software Defined Radio

- Virtex-II FPGA 1M gates
- 2 ch 125Msps A/D and D/A
- TI C6203 DSP
- 32Mbytes SDRAM
- Configurable Digital I/O
- USB 2 or Standalone

### Imaging with Virtex-4FX

- Virtex-4 FPGA FX12
- 128Mbytes DDR Memory
- CameraLink connection
- VHDL and PowerPC Imaging Libs
- USB 2 or Standalone

Programmable hardware with cables, device drivers, loading tools, examples and Power Supply. Systems can be used connected to a PC using USB, or can function standalone (without USB) using the initialisation PROMs.

sales@hunteng.co.uk  
+44 (0)1278 760188  
[www.hunt-rtg.com](http://www.hunt-rtg.com)