

XILINX STORAGE SERVICES

XSS:dm-crypt Acceleration

INTRODUCTION

Xilinx has partnered with Samsung to create the SmartSSD[®] Computational Storage Drive (CSD). This combines a 4 TB Samsung SSD with a powerful Xilinx FPGA to create a high performance and configurable CSD. Loading an accelerator onto the Xilinx FPGA enables the offloading of both the compute that would have been required as well as the data movement between the SSD and this accelerated function.

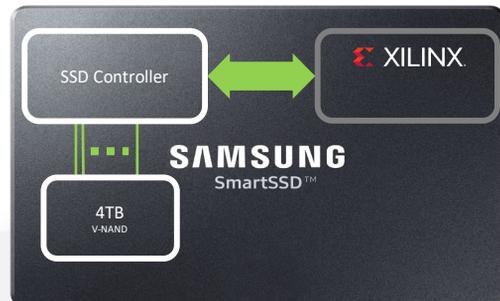
The SmartSSD CSD is a platform that enables different types of computational storage workloads. Xilinx Storage Services (XSS) turns this platform into turnkey accelerated offloads for existing Linux storage software.

PRODUCT OVERVIEW

XSS:dm-crypt accelerates the encryption and decryption of data that is written to or read from the SmartSSD. This provides protection of data-at-rest on the SmartSSD using the AES-XTS-256 encryption standard. This powerful encryption standard is the recommended block cipher mode of the Advanced Encryption Standard (AES) for providing confidentiality of data. It is computationally intensive and provides protection against access of data without a decryption key. This is of high importance in datacenter environments where vast amounts of information are stored, and intentional or unintentional release of data can have dire consequences.

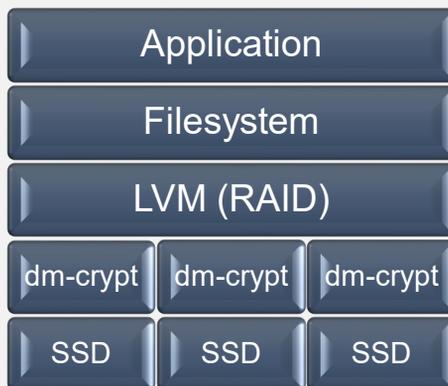
SOLUTION OVERVIEW

DMCrypt is a kernel module in Linux that leverages the device-mapper infrastructure in the Linux kernel. This module maps block IO requests through a transparent encryption function between the IO requestor and the block storage device. By using the device-mapper infrastructure, other storage software can be seamlessly integrated with the dm-crypt module. For instance, a filesystem can be created on an LVM volume that is implementing a RAID protection, with each of the block devices making up the RAID volume having dm-crypt implementing encryption transparently. All these modules are widely available for Linux distribution.



FEATURES AND BENEFITS

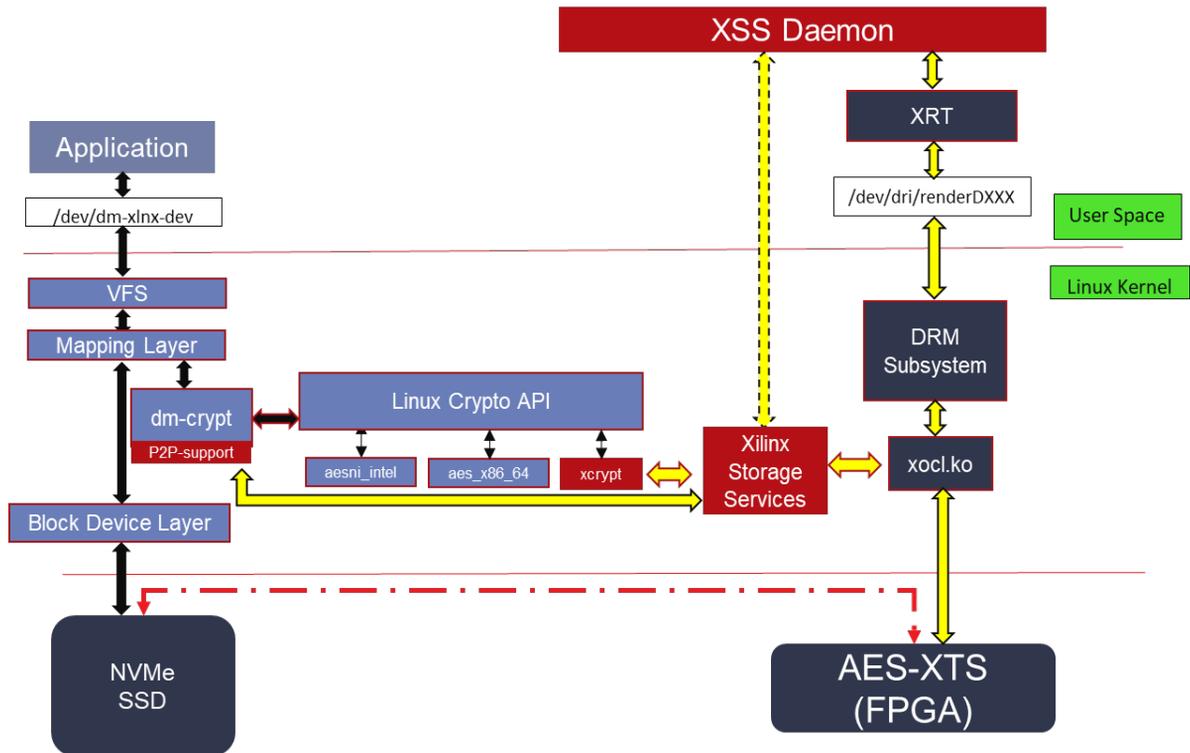
- > Turnkey acceleration of AES-XTS encryption
- > Integration with Linux Device Mapper Crypto software
- > Easy to use off-the-shelf solution
- > Significant CPU offload
- > Acceleration runs directly within the SmartSSD CSD
- > Acceleration scales with the addition of each SmartSSD CSD



Adaptable. **Intelligent.**

XSS:dm-crypt accelerates the underlying encryption function within dm-crypt without requiring any changes to how the dm-crypt module is used. XSS provides a daemon that ensures the FPGA within the SmartSSD CSD is loaded with the encryption acceleration as provides a kernel module that receives storage acceleration API calls. dm-crypt simply leverages these API calls as well as peer-to-peer data transfers to move encrypted blocks to the accelerator.

SOFTWARE APPROACH TO HARDWARE ACCELERATION



XSS leverages the Xilinx Runtime (XRT) that is used to seamlessly bring acceleration to datacenter applications. By augmenting existing Linux storage software, acceleration can be easily leveraged. The SmartSSD CSD presents both the NVMe SSD and FPGA acceleration from the same device, making solutions like XSS:dm-crypt truly turnkey.

CONCLUSION – SIGNIFICANT CPU OFFLOAD

XSS:dm-crypt is a high performance and easy to deploy data encryption solution. As part of Xilinx Storage Services this acceleration is provided free of licensing charges for the SmartSSD CSD. By leveraging standard Linux modules, deploying this solution is no different than deploying the Linux software solution – with the exception that performance is enhanced, and the CPU is offloaded from the heavy encryption/decryption workload.

TAKE THE NEXT STEP

For more information visit www.xilinx.com/smartssd