

Cryptographic Security Leader Boosts Security and Efficiency with Custom Solution



Client Overview

Liquid Security, a series of high performance Hardware Security Modules with a significant presence in the datacenter HSM space, specializes in offloading engines for cryptographic operations, ensuring FIPS compliance.

The Problem

Liquid Security II HSM encountered significant obstacles:



Existing product lacked a distinct control plane, resulting in the mixing of data and control operations within the cryptographic plane.



The new product needed to separate the data and control planes to enhance security and guarantee improved privacy.

The Solution

Bluehatsoft implemented a comprehensive solution, including:

- ✓ Designing two low-bandwidth hardware buses for redundant control command paths, i.e., a Serial Peripheral Interface (SPI) as the primary bus and an Inter-Integrated Circuit (I2C) as the secondary bus for redundancy.
- ✓ Adhering to industry standards using SMBus for the Board Management Console (BMC) interface.
- ✓ Developing hardware interfacing software from scratch and ensuring compatibility with open-source software stacks.
- ✓ Implementing a filtering mechanism in the software stack to reconcile conflicting high level protocol requirements among different buses.

Business Benefits

The implementation of Bluehatsoft's solution resulted in the following:

- ✓ Enhanced security through the separation of data and control command execution paths.
- ✓ Achievement of industry-standard compliance for BMC interface via SMBus.
- ✓ Introduction of newly designed hardware interfacing code and protocol to manage multiple hardware buses efficiently.
- ✓ Fulfillment of client and chip vendor's requirements with tailored software solutions, ensuring optimized performance and reliability.