StrongAuth KeyAppliance

Unprecedented security at an affordable price

- Integrated hardware & software appliance with cryptographic hardware module
- Encryption of structured data-elements: PAN, SSN, PII as well as files of any-type & any-size
- Encryption, Tokenization, Key-Management & Strong Authentication included
- Manage tens of millions of cryptographic keys
- Store billions of encrypted and tokenized data elements
- Integrated to AWS S3, Microsoft Azure & Eucalyptus Walrus for storing encrypted files
- FIDO Certified™ U2F Server for strong-authentication included
- Five (5) FIDO U2F Authenticators included
- FIDO-enabled end-user web-application for file-encryption management included
- High-availability clustering included
- End-to-end encryption for DUKPT processing included
- Secure cloud-computing using the RC3 web-application architecture
- Active Directory, LDAP Server and Oracle Access Manager (OAM) integration included
- Common Criteria EAL4+ Trusted Platform Module (TPM) included - FIPS 140-2 Level 3 certified Hardware Security Module (HSM) option available
- Support for Suite B algorithms
- Hardware-based True Random Number Generator (TRNG) included

StrongAuth, Inc., creators of some of the most innovative open-source Key Management solutions, redefines data-protection once again, bundling encryption, tokenization, key-management and strong-authentication in an affordable, easy-to-deploy, easy-to-use and easy-to-manage appliance.

Application Level Encryption & Strong Authentication

Whether you must comply with PCI-DSS, HIPAA, FISMA, EU Directive or any of dozens of security regulations mandating data-protection worldwide, the StrongAuth KeyAppliance (SAKA) is the first integrated solution to support ALESA* and eliminate a significant portion of the risk of data-breaches.

ALESA eliminates passwords and uses cryptographic keys for strong-authentication using FIDO Alliance** protocols on the front-end. Application level data-encryption on the back-end ensures unauthorized access to sensitive data is denied.

Unlike network-defenses, these two application-security technologies create formidable defenses against the risk of data-breaches leaving attackers - even if inside your network - with no place to go but somewhere else.

Uniquely optimized capability to deliver high levels of security

- A Common Criteria certified cryptographic hardware module to serve as the foundation for securing cryptographic keys – standard. A FIPS certified module is available as an option.
- KeyAppliance Module to manage tens of millions of keys and billions of encrypted and tokenized records
- CryptoEngine Module to encrypt files, digitally sign files and objects, and manage hundreds of millions of FIDO U2F authentication keys
- CryptoCabinet Module to enable end-users to encrypt and store files on public or private cloud-storage while keeping cryptographic keys on-premises
- Data-center class hardware from world-class manufacturers with in-region 24x7 Support for part replacements
- Five FIDO U2F Authenticators to get started with strong-authentication
- Open-source licensing model to eliminate onerous licensing burdens
- Security that exceeds regulatory requirements for PCI-DSS, HIPAA and other security regulations

* https://alesa.website/ ** https://fidoalliance.org/

Specifications

Form Factor	2U
Central Processing Unit	8-core 64-bit (Capacity up to 2 CPUs)
Memory	32 Gigabytes PC3-12800R (Capacity up to 768GB)
Hard Disk Drive	2 x 1TB 6G SAS 7200 RPM 3.5" with Hardware RAID-1 (Capacity up to 10TB)
Networking	Quad-port, 1 Gb Ethernet
Power Supply	2 x 460W at 100V to 120V AC input 2 x 460W at 200V to 240V AC input
Ports	VGA, USB
Remote Management	Dedicated integrated Lights Out (iLO) port
Cryptographic Hardware	Trusted Platform Module v1.2/v2.0 (Common Criteria EAL 4+) Hardware Security Module (PCIe – FIPS 140-2 Level 3)
Dimensions H x D x W	8.73 x 74.93 x 44.55 cm (3.45 x 29.5 x 17.54 in)
Weight	27.27 Kg (60.12 lb) (Maximum) 21.36 Kg (47.10 lb) (No drives installed)
Rails	Easy Install Rail Kit

Operating System	64-bit CentOS Linux
Relational Database	MariaDB (MySQL)
Application Server	Java Enterprise Edition 7 (Glassfish, TomEE, WildFly)
Messaging	JeroMQ
Cryptography	BouncyCastle, Trusted Java, CryptoServer JCE
Directory Server	OpenDJ
StrongAuth Software	Key Appliance Module CryptoEngine Module CryptoCabinet Module

StrongAuth, Inc. 10846 Via San Marino, Cupertino CA 95014-6333 USA
Phone: +1 408-331-2000 E-mail: sales@strongauth.com Web: http://www.strongauth.com/