

# STRONGKEY

## HIGHLIGHTS

- 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® Server for strong authentication included
- Five (5) FIDO authenticators included
- High-availability clustering included
- End-to-end encryption for DUKPT processing included
- Active Directory and LDAP Server and Oracle Access Manager (OAM) integration included
- FIPS 140-2 Level 2 TPM included
- FIPS 140-2 Level 3 HSM option
- Support for Suite B algorithms
- Hardware-based True Random Number Generator included

## Tellaro™ E1000 – Enterprise Solution

UNPRECEDENTED SECURITY AT AN AFFORDABLE PRICE

*StrongKey, 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 (ALESA)

Whether you must comply with PCI DSS, HIPAA, FISMA, GDPR, or any of dozens of security regulations mandating data protection worldwide, or you are looking ahead to regulations like CCPA, and others, the StrongKey Tellaro E1000 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 frontend. 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.

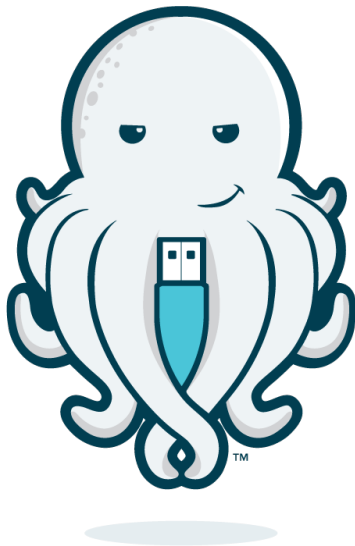
## UNIQUELY OPTIMIZED CAPABILITY TO DELIVER HIGH LEVELS OF SECURITY

- A FIPS 140-2 Level 2 Trusted Platform Module (TPM) cryptographic hardware module to serve as the foundation for securing cryptographic keys is included
- A FIPS 140-2 Level 3 certified Hardware Security Module (HSM) is available as an option
- Built-in module to manage tens of millions of keys and billions of encrypted and tokenized records
- Built-in module to encrypt files, digitally sign files and objects, and manage hundreds of millions of FIDO authentication keys
- Data center-class hardware from world class manufacturers with support for part replacements
- US-based support M-F included, with 24x7 support option
- Five (5) 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, GDPR, and other security regulations



## SPECIFICATIONS

Form Factor	1U or 2U
CPU	8-core 64-bit
Memory	32 Gigabytes
Networking	Dual-port, 1 GB Ethernet
Hard Disk Drive	2 x 1TB 6G SAS 7200 RPM 3.5" with Hardware RAID-1 (Capacity up to 10TB)
Ports	VGA, USB
Cryptographic Hardware	TPM 2.0 (FIPS 140-2 Level 2 certified) included HSM (PCIe - FIPS 140-2 Level 3 certified) optional
Dimensions W x D x H	8.73 x 74.93 x 44.55 cm (3.45 x 29.5 x 17.54 in)
Weight	27.27 Kg (60.12 lbs.) (Maximum) 21.36 Kg (47.10 lbs.) (No drives installed)
Rails	Easy Install Rail Kit
Remote Management	Dedicated integrated Light Out (iLO) port/DRAC port
Power Supply	2x 460W at 100V AC input 2x 460W at 200V to 240V AC input
System Software	SecureOS™ open-source security operating system



### ABOUT STRONGKEY

**StrongKey makes data breaches irrelevant** by redefining how businesses and government agencies secure their information against the inevitability of a breach. While other security companies focus on protecting the perimeter, StrongKey secures the core through strong authentication, encryption, digital signatures and hardware-backed key management—keeping the core safe even with an attacker on the network. Based in Silicon Valley, CA and Durham, NC, StrongKey has provided cryptographic security solutions for over 17 years and is trusted in mission-critical business operations by some of the largest companies in payment processing, e-commerce, healthcare, and finance. Learn more at [www.strongkey.com](http://www.strongkey.com).

#### StrongKey

Durham, NC & Cupertino, CA

Phone: +1 408-331-2000 | E-mail: [getsecure@strongkey.com](mailto:getsecure@strongkey.com) | Web: [strongkey.com](http://strongkey.com)

©2018 StrongAuth, Inc.. All Rights Reserved.

Information subject to change without notice.