EKA | CyberLock®

COMMUNICATION DEVICES
Validikey 20 vault

Part number: CKV-V20

Communicators underpin the flexibility of EKA CyberLock. Simple, instant key activation.

Increase Key Control & Accountability
Automate process of checking in/out CyberKeys

Manage Access to Outside Vendors
Dispense temporary access or one-time use CyberKeys

Securely Store Keys on Site
Perfect for high security buildings

The VALIDIKEY 20 Vault can function as a stand alone system, or it can be scalable, meaning numerous vaults can communicate within a single CyberAudit® Enterprise system.

The VALIDIKEY 20 Vault reads the ID of most un-encrypted 13.56 MHz RFID cards, secures 20 CyberKeys, supports Generation 2 Keys, and recharges CyberKeys while in the vault. The front of the vault contains an RFID reader with an indicator light, a keypad, and an LCD touch screen that displays status.

VALIDIKEY™ 20 Vault

Part number: CKV-V20

The VALIDIKEY 20 Vault is a key cabinet designed to program and dispense up to 20 keys. The keys are stored in the secured vault in an unprogrammed state until an approved PIN or RFID card is presented. After the presentation of an approved PIN or RFID card the vault programs a key with that user's access permissions and releases the door latch.

Specifications

Physical	Black powder-coated aircraft-grade aluminum case; aluminium door, latch tested to 1200 lbs. (544kg)
Operating Temperatures	32°F to 122°F; 50°C; non-condensing; indoor or sheltered installations only.
Dimensions	16.3" H x 12.2" W x 4.6" D (414mm x 310mm x 117mm)
Weight	16lbs. (7.3kg) Does not include keys.
Power	**Input**-100-24O VAC I.5A 50-60Hz.
	Output-19V DC 3.42A center-positive pin.
User Panel	12 key keypad allows entering of a PIN for issuing keys; RFID reader. Touch display screen for displaying status
Sound	Low volume beeper in RFID reader; high volume Piezo buzzer in vault.
Memory	1GB RAM and 4GB storage for settings, key configurations, and audit trail storage.
Compatible RFID Cards	Reads the unique ID from unencrypted 13.56MHz ISO 14443 Type A and B, and ISO 15693 format cards (i.e. I-Code, Mifare, Legic). Custom Weigand reader option.
Software Option 1:	Operates as a stand-alone system for managing up to 20 Gen 2 CyberKeys.
Software Option 2:	Operates as a communicator in a CyberAudit® Enterprise system with the ability to utilise Gen 2 keys, CK-RXD, and CK-RXD2.

How it works

8:00am 🕐

20 CyberKeys are stored in the vault in an unprogrammed state. Users present a PIN or RFID to the VALIDIKEY 20 Vault.

5:00pm 🕐

To return a CyberKey to the vault the key user presents their PIN and/or RFID to open the vault. After opening the vault users may return their CyberKey to any available slot.

8:01am 🕐

The vault communicates with the CyberAudit® software. The software programs a key with access permissions and then allows the vault to open. The programmed CyberKey is now available to be removed from the vault.

5:01pm 🕐

The vault communicates both vault and CyberKey activity to the CyberAudit® software.

8:02am - 5:00pm 🕐

The CyberKey user can now go about their day opening locks that their key is programmed to open.

5:02pm 🕐

The software manager receives an automated email containing the audit report for that day.