FUTUREX

FUTUREX KEYLINX

PCI PTS Certified
Platform For Controlled
Key Ceremony Workflows

Secure, Remote Key Management

Remotely Load Your Encryption Keys - On-Premises And Cloud

The Futurex KeyLinx is a PCI PTS certified handheld key loading device that enables authorized operators to perform key ceremonies on remote Futurex devices from a portable, touch-based interface.

It eliminates the need for in-person data center visits for routine key loading ceremony execution - delivering the same rigorous procedural controls required by compliance frameworks in a device built for secure key loading operations.

Core Specifications

Physical Specs
- 3.23 x 8.11 x 2.40 in; 1.11 lb
- 5.4 inch multi-touch color display, 720 x 1440 px

Validation / Certification
- PCI PTS

Algorithms supported
- 3DES
  - Double-length 3DES key: 32 hex characters
  - Triple-length 3DES key: 48 hex characters
- **AES**
  - AES-128: 128-bit strength
  - AES-192: 192-bit strength
  - AES-256: 256-bit strength

Futurex devices supported
- CryptoHub
- Excrypt HSM platform (2026)
- Excrypt Plus/Enterprise (prior generation
- Vectera Plus
- VirtuCrypt

The Challenge

Cryptographic key ceremonies to load keys into HSMs are among the most sensitive, compliance-critical procedures an organization runs. Traditionally, they required all key custodians to be physically present at the same device, in the same location - usually a secure data center - at the same time. For organizations with distributed teams or multiple sites, this is a logistical and cost burden.

Additionally, regulatory frameworks like PCI PTS impose specific control objectives around how key material is handled, loaded, and protected. Every Futurex product - Excrypt HSM, CryptoHub, and VirtuCrypt cloud - utilizes a Platform Master Key (PMK) that encrypts all other keys used by the system. Loading, escrowing, and recovering that key securely requires a certified, external Secure Cryptographic Device (SCD).

WHAT DOES THE FUTUREX KEYLINX DO FOR YOU?

The Futurex KeyLinx gives authorized operators a secure, portable means of executing key ceremonies from any location - without requiring physical data center access for routine procedures.

Maintains Rigorous Security

- Key components are never transferred as clear text.
- Every Futurex KeyLinx is digitally signed with your organization's root certificate, ensuring only your device accesses your Futurex infrastructure.
- The Futurex KeyLinx connects to a workstation over a mutually authenticated, encrypted session and leverages TR-31 and TR-34 to securely perform key loading operations.
- Dual-factor authentication and dual-login requirements protect access to the configuration application.
- Key component entry occurs in separate steps, each with its own check digit display, enforcing split knowledge procedures.

Reduces On-Site Visits

- A single Futurex KeyLinx can load keys to Futurex devices across geographically dispersed sites, eliminating routine in-person visits for key loading, configuration, and updates. It reduces travel, scheduling complexity, and the operational cost of managing distributed cryptographic infrastructure.

Meets Compliance Requirements

- Futurex KeyLinx is certified under PCI PTS as an SCD, satisfying control objectives for key loading and device management.
- Provides authenticated audit logs of all activity and access, simplifying audit management.

Optimizes Operational Costs

- Reduces travel, on-site servicing, and operational support requirements for routine key management.
- Enables remote key loading to reduce downtime and improve cryptographic operations efficiency.

Your Remote Management Ecosystem

The Futurex KeyLinx is the device-level component of a broader remote management solution. It supports remotely loading initial keys into Futurex devices, enabling lights-out HSM deployments. In practice, you can ship a unit directly to the data center, remote staff rack-and-stack and assign an IP address, then the full configuration - including loading the initial major keys - can be completed remotely through secure web portals.

This gives teams visibility and control across distributed deployments while reducing operational overhead and maintaining consistency, auditability, and compliant security. Combined, the Futurex KeyLinx and Futurex's suite of on-premises and cloud HSMs create a more scalable model for managing cryptographic operations across multiple sites and environments.

Use Cases

PMK Escrow & Recovery

- Every Futurex product relies on a Platform Master Key (PMK) that encrypts all other keys on the system. If it's lost, the system cannot function.
- The Futurex KeyLinx is a secure, compliant mechanism to back up and recover the PMK - via XOR components or M of N smart card shares.

Payment Key Interoperability

- Every entity in the payment chain shares encryption keys - the Futurex KeyLinx loads those keys from externally provided components, in a PCI-compliant manner, with each component entered by a separate custodian.
  Supports PEKs, DUKPT BDKs, and other payment keys across the transaction ecosystem - and works with CryptoHub to manage ceremonies and key delivery at scale.

Controlled Key Workflows

The Futurex KeyLinx guides operators through repeatable, procedurally compliant workflows via its touch-based interface without requiring specialized expertise at every step. Each workflow enforces the security controls and audit trail required for sensitive key operations, while reducing the complexity and error risk of manual processes.

Additional supported workflows include:

- Key ceremony execution across separate locations and separate times
- Secure key loading operations from components or smart cards
- Multi-operator approval procedures
- Administrative authorization workflows

Futurex Integration

The Futurex KeyLinx is Futurex's dedicated key loading device, designed to securely load keys into supported Futurex devices and services. Paired with VirtuCrypt's global network of over a dozen data centers, it supports remote key loading into distributed Futurex devices and services without requiring on-site visits.

Futurex's remote management portals, including the HSM portal, CryptoHub portal, and VIP Dashboard, provide the centralized administration, monitoring, and configuration capabilities that support comprehensive remote operations.

Specifications

Physical & Environmental

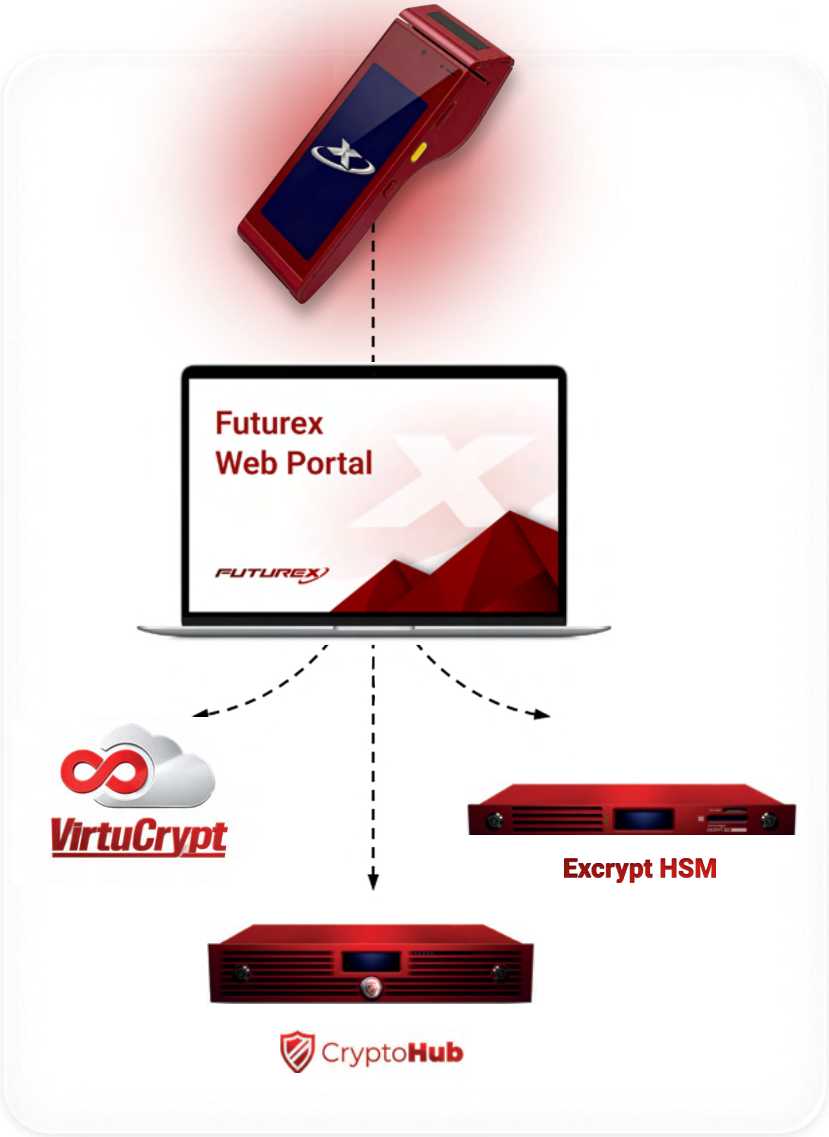
Durability:
Drop tested to 1.2 m (faces and edges)

Ports and slots:
USB Type-C

Environmental:
Operating: -10°C to 50°C, 10 to 90% RH
Storage: -20°C to 70°C, 10 to 90% RH

Power and battery:
USB Type-C multi-voltage adapter
DC 5 V via USB or contact pins
7.4 V 2600 mAh rechargeable Li-ion

Included in box
USB Type-A to USB Type-C cable
Optional USB Type-C power adapter
Optional USB-C to USB-C cable



For over 40 years, Futurex has been an award-winning leader and innovator in the encryption market, delivering uncompromising enterprise-grade data security solutions. Over 15,000 organizations worldwide trust Futurex to provide groundbreaking hardware security modules, key management servers, and cloud HSM solutions.

Futurex is headquartered outside of San Antonio, Texas, with regional offices worldwide and over a dozen data centers across five continents. Futurex delivers unmatched support for its clients' mission-critical data encryption and key management requirements.

FUTUREX.COM

864 Old Boerne Road,
Bulverde, Texas 78163