

FUTUREX SECURUS

A Portable, Touch Screen-Based Key
Generation and Loading Device

GENERAL-PURPOSE DATA ENCRYPTION



A Secure, Robust, and Portable Solution

The Securus combines the convenience of a touch screen-based tablet with Futurex's world-renowned data encryption and security technology to create a truly revolutionary solution for key generation, loading, and storage.

With the Securus, previously complicated and lengthy procedures for key management are reduced to simple point-and-click activities with even greater protection against security threats.

The device's extensive array of key management capabilities are matched only by its ability to serve as a single point of configuration for multiple geographically-diverse systems. Network-connected Futurex solutions from around the world can be managed using a single Securus.

Eliminate the Difficulty and Cost of Key Management

Integrated smart card support allows you to transition away from paper-based key component storage. Each smart card functions as an individual Tamper-Resistant Security Module, allowing storage of clear key components. By using smart cards, you gain peace of mind over your key transfer process by ensuring that your sensitive data will have industry-certified safeguards against tampering.

Regulatory requirements stating that encryption keys must be loaded using a compliant Key Loading Device are fully satisfied by the Securus. The Securus is a FIPS 140-2 Level 3-validated Tamper-Resistant Security Module and can be connected directly to older devices which are not equipped with smart card hardware.

Remote Device Configuration and Key Loading

Spending significant amounts of time in a data center used to be a necessity for establishing and maintaining a payment processing or key management infrastructure. With the Securus, networked Futurex devices may be configured from anywhere, via a secure connection.

Organizations with multiple backup or disaster recovery sites are able to use a single Securus from a single location to manage most network-connected Futurex devices. Travel time is reduced, data center access is kept to an absolute minimum, and updates are able to be delivered quickly and effectively across your entire infrastructure.

A Portable, Dedicated, and Compliant Key Generation and Loading Device

- Complies with regulatory requirements for compliant key generation, transport, and entry
- Simple touch screen-based point and click interface
- Reduces the cost and inconvenience of transporting keys
- Allows for secure, remote configuration and key loading for Futurex Hardware Security Modules and Key Management Servers

FUTUREX.COM



The Futurex Securus will help you streamline and increase the efficiency of your payment processing, key management, and general-purpose data encryption infrastructure.

Cost-Effective Solutions

- Eliminates the costly manual process of transferring key components
- Capable of configuring multiple devices for the management of a full range of encryption security solutions
- Eliminate the need to schedule data center visits for device configuration and maintenance
- Easily manage your worldwide data encryption presence from a single location

Simplified Usage

- Easy to use GUI helps reduce training and requirements for operators
- Integrated touch screen and smart card reader eliminates the need for cumbersome peripherals
- Large, high-resolution screen designed for clarity, responsiveness, and functionality
- Intuitive controls allow operators to quickly shift between modes of operation

Industry Compliant Standards

The Securus meets and adheres to the following compliant standards:

- FIPS 140-2 Level 3
- ANSI X9.24 part 1 and part 2—TR-39
- RoHS
- FCC Part 15 - Class B

PKI-Based Remote Functionality

- Configure and load encryption keys into most network-connected Futurex devices both locally and remotely
- Remotely generate cryptograms
- Establish a secure, signed connection with Futurex devices for dual-factor authentication using smart cards
- Create a bridge connection for injecting remote or offline Encrypting PIN Pads (EPPs)

Powerful Logging Capability

- Provides detailed audit records in a convenient, exportable format
- Simplifies management of internal and external TR-39 audits
- Complete, authenticated audit log files of all activity and access

Uncompromising Physical Security

The Securus contains the following physical security features:

- Hardened aluminum case with full tamper-resistant functionality
- Tamper resistant security module (TRSM) with opaque barrier and sensor wires to protect processor and system memory
- Battery backup for encryption keys stored in TRSM memory

Robust Logical Security

- Dual logins required to access key loading application
- Dual-factor authentication for increased security
- User group permissions control privileges within key loading application
- Keys are stored as cryptograms under the master file key of the key encryption key
- Key component entry occurs in separate steps each with own check digit display