

# FUTUREX Certificate Authority Server

GENERAL-PURPOSE DATA ENCRYPTION

A Complete, Hardware-Based Certificate Authority Solution



## A Complete, Hardware-Based Certificate Authority Solution

- Secure, robust certificate creation and storage
- Sign code, patches & updates, and individual devices
- Track and export certificate revocations through built-in Certificate Revocation List
- Integrated, hardware-based disaster recovery and redundancy features
- Customized alerting via SMTP, SNMP, and SMS when integrated with the Guardian9000
- Robust, permission-based user management system for separation of duties
- Capable of bringing total system redundancy and disaster recovery capabilities to your certificate authority infrastructure
- Advanced feature set prepares your organization for future regulatory changes and updates
- PKI-based remote Master Key loading for Lights-Out datacenters using the Futurex Securus

## A Complete, Hardware-Based Certificate Authority

The Certificate Authority Server provides a robust, easy-to-use solution for creating and storing asymmetric key pairs to encrypt/decrypt and sign/validate anything that relies on a Public Key Infrastructure.

### Examples of this include, but are not limited to:

- Establishing SSL connections
- Authentication of individual electronic devices or documents
- Communication encryption
- Secure distribution of symmetric keys

It can also be used to sign data with trusted PKI keys to ensure data integrity. It can manage the entirety of the process, from creation of a self-signed root certificate and management of the subordinate certificate tree and asymmetric key pairs to management of a Certificate Revocation List.

## Security and Regulatory Compliance

A FIPS 140-2 Level 3-validated Tamper Resistant Security Module (TRSM) is incorporated into the key generation and loading process, providing dependable security. The device stores all required tracking and serial number information, allowing easy traceability for auditing requirements. The Certificate Authority Server follows all the required ISO, ANSI, FIPS, and PCI DSS regulatory requirements.

## Seamless Integration

The Futurex Certificate Authority server is designed to function as a complementary product to numerous other Futurex devices, including the Remote Key Management Server and Kryptos TLS Server, allowing you to standardize on the Futurex platform.

For organizations wishing to implement the Certificate Authority Server into environments with other proprietary devices already in production, our TR-39-certified Solutions Architects are highly experienced in crafting total turnkey solutions that allow you to seamlessly integrate our devices into your existing data encryption infrastructure.

## SPECIFICATIONS

# Certificate Authority Server

### Dimensions & Weight

Space: 2U  
Weight: 36 lbs (16.3 kg)

### Meets Industry Compliance Standards

FIPS 140-2 Level 3  
ANSI X9.24 part 1 and part 2 for Symmetric and Asymmetric Key Management — TR-39  
RoHS  
FCC Part 15 – Class B

### Operating Conditions

Power requirements: 100 - 230 VAC 50/60 Hz. 400 Watts  
Operating temperature: 50° to 95°F (10° to 35°C)  
Storage temperature: -40° to 149°F (-40° to 65°C)  
Operating relative humidity: 20% to 80% non-condensing  
Storage relative humidity: 5% to 95% non-condensing

### External Hardware Requirements

Keyboard: Standard USB  
Mouse: Standard USB  
Video: SVGA 1024x768 at 75Hz refresh

### Hardware Redundancy

Dual, redundant, hot-swappable power supplies  
Dual, redundant Ethernet ports  
Failover link with additional Certificate Authority Server units using the Guardian9000

### Securus-Based Remote Management Capabilities

Master Key loading  
User and permissions administration  
Log management and audit reporting  
Synchronization of keys and configuration details across multiple Certificate Authority Server devices  
Firmware distribution and installation

### Certificate Authority Server Unit Includes

Certificate Authority Management application CD  
User guide  
Mounting brackets  
Two TRSM barrel keys  
Cables

## Stay organized and secure with the comprehensive, hardware-based security and functionality of the Futurex Futurex Certificate Authority Server

### Functionality

- Generates asymmetric key pairs for use in encrypting/decrypting and signing/validating data
- Signs software code, firmware updates, digital signatures, and SSL connections
- Integrates with the Futurex RKMS Series for remote injection of Encrypting PIN Pads for ATM and POS environments
- Capable of tracking and exporting certificate revocations through a built-in Certificate Revocation List

### Industry Compliant Standards

The Certificate Authority Server meets and adheres to the following compliant standards.

- PCI DSS
- FIPS 140-2 Level 3
- ANSI X9.24 part 1 and part 2 — TR-39

### Uncompromising Physical Security

The Certificate Authority Server contains the following physical and logical security features:

- 2U hardened steel interlocking rack mounted case
- Two unique face-plate bezel locks for securing the server to the rack
- Tamper resistant security module (TRSM) with epoxy barrier and sensor wires to protect processor and system memory
- Battery backup for keys in TRSM memory
- Multi-user grouping for access restriction

### Robust Logical Security

- Dual logins required to access certificate application
- Adjustable user control privileges within certificate application

### Audit Tracking Capability

- Provides detailed audit records and the ability to generate certificate reports
- Easily manage internal and external audits
- Stores all tracking information and certificate authority activity for auditing requirements
- Maintains complete, authenticated audit log files of all activity and access

### Ease of Use

- Easy to use GUI helps reduce training and requirements for operators.
- Quickly supports large certificate tree creation and signature batches
- Allows for a simplified method for certificate creation
- Certificates can be exported in PKCS7 or X509 formats with DER or PEM encoding, or in PGP format.
- User group permissions control privileges within certificate application

### Secure File Signing

- Files can be digitally signed by the Certificate Authority Server using the SHA1 or PGP algorithms.
- The Certificate Authority Server can expand .tar files, sign individual files within the archive, and then recompress it with the signature of the chosen file(s).
- Digital signing can ensure the integrity of the file so that it can be transferred with the assurance it has not been tampered with.

### Fully Automated, API-Driven Interface

- Includes full Host API functionality for the programmatic automation of repetitive tasks
- Versatile, extensible command structure allows additional functionality to easily be incorporated
- Ideal for large-scale implementation of digital signature operations
- Full turnkey solutions to fit unique environment needs may be developed with the assistance of the Futurex engineering team