

# FUTUREX Certificate Authority Server

GENERAL-PURPOSE DATA ENCRYPTION

A Complete Certificate Authority Solution  
for Your POS or ATM Network



## 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
- PIN Pad key injections
- Communication encryption
- Remote Key Management Server connections

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-certified 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.

### A Complete Certificate Authority Solution for Your POS or ATM Network

- Secure, robust certificate creation and storage
- Sign code, patches & updates, and individual devices
- Track and export certificate revocations through built-in Certificate Revocation List

## SPECIFICATIONS

# CA Server

### Operating System

Secured Linux

### Dimensions & Weight

Space: 2U

Weight: 36 lbs (16.3 kg)

### Meets Industry Compliance Standards

PCI DSS

FIPS 140-2 Level 3

ANSI X9.24 part 1 and part 2 for Symmetric and Asymmetric Key Management — TR-39

### 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 PS/2

Mouse: Standard PS/2

Video: Standard PS/2 SVGA1024x768 at 75Hz refresh\*

\*Note: the refresh is high speed and may not work with older monitors

### Certificate Authority Server Unit Includes

Certificate Authority Management application CD

User guide

Mounting brackets

Two TRSM barrel keys

Cables

## Stay organized and secure with Futorex 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 Futorex Remote Key Management Server 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 is a FIPS 140-2 Level 3 validated hardware security device with the following physical 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.

**NORTH AMERICA—Global Headquarters** 864 Old Boerne Road, Bulverde, Texas 78163  
TF 800.251.5112 P 830.980.9782 F 830.438.8782 info@futurex.com

**EUROPE** 2430/2440 The Quadrant, Aztec West, Almondsbury, Bristol, BS32 4AQ UK  
P+44 (0) 1454 877681 info.intl@futurex.com

**ASIA** One Fullerton, One Fullerton Road, #02-01 One Fullerton, Singapore 049213  
P+65 6832 5176 info.asia@futurex.com

**WWW.FUTUREX.COM**

**FUTUREX**