# Powerful and innovative security for remote network access

TOSIBOX® Lock 500 is a powerful and sophisticated VPN endpoint capable of securing links between remote users and small to medium enterprise networks.

TOSIBOX® Lock 500 features a range of new connectivity and security features including optional built-in LTE (cellular) modem for instant remote connection, innovative digital I/O ports which can be used for sophisticated control and monitoring of the Lock 500's operations in critical environments, and improved VPN throughput. Behind the scenes the Lock 500 includes new security features that harden the firmware through secure boot and new cryptographic key handling technologies.

Like its predecessors, the Lock 500 uses Tosibox's physical Key and Lock model. This means access to sensitive and secure network assets is restricted to users that are able to physically present a secure USB key and know the password for it. Two-factor authentication (2FA) is recommended by all current security standards and organisations such as ISO27002, NIST, ETSI, and the latest PCI DSS.

The use of multi-factor authentication greatly improves network security as attackers are unable to brute force passwords without access to a physical Key device, and conversely, the loss of a physical Key does not immediately compromise the network as the Key's password is also required.

## Innovative security features

TOSIBOX® Lock 500 incorporates new and innovative security features including a user-customised digital I/O interface; new firmware security measures including secure boot architecture, up-to-date operating system components, kernel and module code signing; plus, the use of a secure hardware crypto-processor embedded inside the CPU to physically restrict access to sensitive encryption and signing keys.

## Digital input/output interface

The digital input/output interface provides advanced control and monitoring features for the TOSIBOX® Lock 500. These digital I/O 'pins' can be connected to physical switches, signals, and alerting mechanisms.

By configuring I/O pin behaviour, the Lock 500 can be brought online (or taken offline) by external events. For example, the Lock 500 could be configured to wait in a securely isolated offline state (preventing all remote network access), it can then activate the VPN connection in response to physical changes such as the turn of a key-switch, activation of a motion-detector relay, or an externally generated alarm (from an industrial control system). The output pins may be used to provide visual or audible alerts for events such as Internet connection failures, and VPN state changes. These alerts could provide immediate warnings to staff or feed in to other security or monitoring systems.

The digital I/O port allows TOSIBOX® Lock 500 end-users to develop their own innovative and powerful security processes and controls.

## Firmware security with secure boot and kernel signatures

Critical to device security is the ongoing maintenance and support of built in firmware. While many consumer and small-business routers feature obsolete kernels and drivers, TOSIBOX® Lock 500 has been developed for enterprise users using the latest 'long term support' kernels, and is actively maintained and managed through Tosibox's audited security practices. This means that the Lock 500 firmware is actively updated and patched against current known vulnerabilities and threats.

The Lock 500 features new security hardware, which allows encryption and signing keys to reside in the CPU's internal secure key-store of the embedded crypto-processor. Tosibox uses these security features to embed firmware signing keys in to the Lock 500 hardware. This means the quality, reliability and security of TOSIBOX® firmware releases are assured, because no malicious or third party modules can be installed on to the Lock 500.

This chain of integrity is maintained from the very moment the Lock 500 is powered on; a secure boot loader checks the validity and signature of the kernel and other resources before allowing the system to start. This means the Lock 500 can be placed in uncontrolled network environments – for example as part of a service contract or security monitoring solution – where the Lock 500 owner has no physical control over the device's security.

Even in hostile environments, attackers are limited as to what they can achieve because secure boot and code signing eliminates the risk of the box being 'rooted' or manipulated by malicious third parties.

**Finland**
sales@tosibox.com
support@tosibox.com
Sales, Finland Tel. +358 44 709 0100
Sales, International Tel. +358 44 709 0200
www.tosibox.com

**United States**
Tel. +1 678 478 5056

**Germany**
Tel. +49 6106 63 94 172

**Scandinavia**
Tel. +46 73 625 4555
Tel. +46 70 646 5017

TOSIBOX®

## Hardware enforced confidentiality of keys

TOSIBOX® Lock 500 incorporates a secure key store and crypto-processor embedded in the CPU. This secure crypto-processor improves on traditional encryption systems and software VPNs because the secret keys are physically isolated from the rest of the system.

In an ordinary software VPN, an administrator must generate public and private keys that are used to authenticate users and sign session keys and other critical data. When key material is generated and used in user-space, the material is susceptible to leakage through direct file system access, unsecured backups, or even malicious exfiltration. The VPN's security is entirely contingent on the integrity of these encryption keys and digital signatures – it is vital that these keys are handled carefully.

By contrast, an embedded secure crypto-processor in all TOSIBOX® Lock 500 devices completely isolates sensitive cryptographic keys from the rest of the system.

The crypto-processor embedded in the Lock 500's CPU provides hardware-enforced confidentiality of sensitive cryptographic material. Instead of accessing the secret key from the device mass storage or memory, the TOSIBOX® VPN application instructs the CPU to encrypt, decrypt, sign and verify secure messages. This means users, applications, and not even the operating system can access the secret key data.

Because the key material is never accessible, Lock 500 VPN connections are secure from attack from even the most sophisticated adversary – there is simply nothing for the attacker to steal. The use of hardware-enforced confidentiality further improves the Lock 500's resilience in hostile or uncontrolled network environments.

## Summary

TOSIBOX® Lock 500 represents a new level of security and assurance in the management and maintenance of secure network environments. The Lock 500 incorporates innovative new features that allow the Lock 500 to be integrated with external security mechanisms and monitoring solutions. The device firmware and VPN keys have also been hardened for use in hostile and uncontrolled environments, protecting the device and network from attacks by hackers, malicious users and malware.

The innovative digital I/O pins allow small business and enterprise users to enhance or develop their own security controls and monitoring solutions on top of the Lock 500's secure access technology.

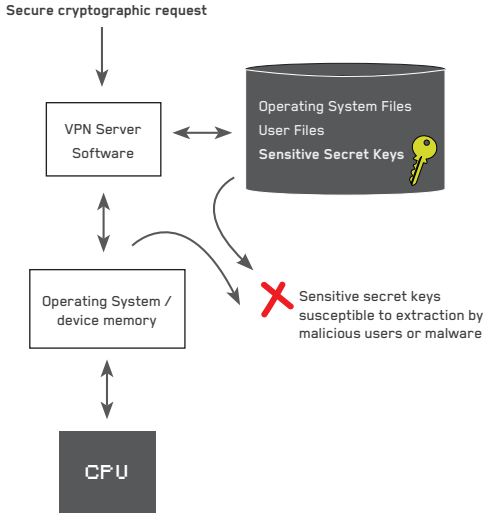
The secure boot and code signing features have hardened the Lock 500 against malicious attacks and modification of key firmware components.

The secure hardware-based crypto-processor has eliminated the risk of secret key compromise even in hostile and uncontrolled or hostile environments where attackers may have physical access to the Lock 500 device.

## Overview of digital signing process and secret and availability

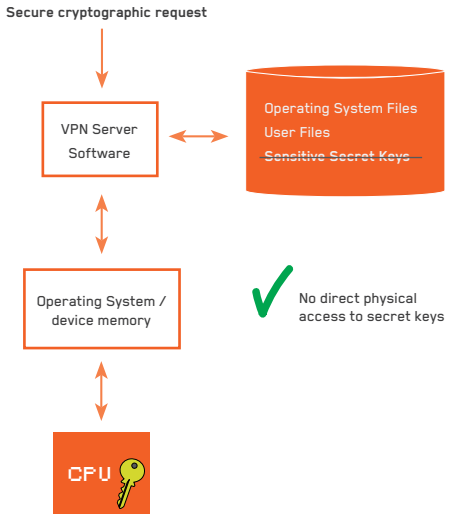
**Traditional software based VPN without embedded hardware cryptoprocessor**

- Secure message is hashed (Message Digest created)
- Private key is retrieved from the filesystem and stored in memory
- Private key is applied to the Message Digest by the VPN Server software
- The publicly safe signature is sent along with request data




**TOSIBOX® Lock 500 - utilizing hardware security to eliminate access to secret keys**

- Secure message is hashed (Message Digest created)
- Software requests the CPU to sign the Message Digest
- CPU uses isolated secret key to sign the Message Digest
- The publicly safe signature is sent along with request data





**Finland**
sales@tosibox.com
support@tosibox.com
Sales, Finland Tel. +358 44 709 0100
Sales, International Tel. +358 44 709 0200
www.tosibox.com

**United States**
Tel. +1 678 478 5056

**Germany**
Tel. +49 6106 63 94 172

**Scandinavia**
Tel. +46 73 625 4555
Tel. +46 70 646 5017


TOSIBOX®