TOSIBOX INFORMATION SECURITY

TOSIBOX builds networks with strong encryption over public infrastructure such as mobile networks. Data is encrypted and decrypted in the TOSIBOX® products at the connection end points, e.g., at the edge Node or Virtual Central Lock and the user Key. There are no intermediate servers or users that can decipher the information transmitted in the connection. The highly encrypted data stream transmitted over the Internet is readable only at the end points.

TOSIBOX protects *data confidentiality* by encrypting information as it is transmitted over insecure medium. TOSIBOX® protects *data integrity* by verifying information is in unaltered state when received at the end point. TOSIBOX® protects *data availability* by providing always-on VPN tunnels for authorized users.

TOSIBOX is audited, patented, and performs at the highest security standards in the industry to provide unsurpassed level of information security. The technology is based on globally acknowledged information encryption standards, secure user authentication, automatic security updates and simplifying often complex technology.

Tosibox Devices

TOSIBOX® Key is an intelligent USB-connected device that contains a secure cryptoprocessor. The Key is used to establish a secure connection to the edge Node. All TOSIBOX® Keys and edge Nodes are interoperable. TOSIBOX® Key can be a Master Key that is the top authority to manage the network access rights for other Key user. Key users can be software only Keys, hardware Keys or Mobile Client users.

TOSIBOX® Node is a device that accepts remote connections from Keys and creates private and secure access to connected network devices. The network devices that are connected to the Node´s LAN port are automatically discovered. Node can also be connected together to expand a single network to multiple sites. When connecting two Nodes to each other, one must be in Sub Lock mode of operation where the Node is a subordinate to its master Node.

TOSIBOX® Virtual Central Lock is a VPN tunnel concentrator that maintains always-on VPN connections towards TOSIBOX® Nodes and provides centralized user and network management.

Device Identities

TOSIBOX® products identify each other by cryptographic pairing in which the products are matched with each other before use. This is achieved locally by connecting the TOSIBOX® Node with the user Key physically, or remotely by generating the Remote Matching Code on the device that is to be matched.

In the physical matching process, the Key device is inserted into the USB port of the edge Node. In Remote Matching the device that is to be matched generates a cryptographic code that can be entered in the Key SW. In the matching process, the edge Node and Key exchange public key of the keypair with each other to create a mutual trust relationship. The encryption key is stored in a closed memory location of the crypto processor on the Key device. The encryption key is protected with a password even if you lose the Key device. The encryption key cannot be copied or tampered with by outsiders. Establishing a remote connection to the edge Node is impossible without the correct encryption key.

Key Connection

Every user Key uses either a bridged Layer 2 or a routed Layer 3 connection. The Layer 2 connection type means that the edge Node is essentially in the same network with the user that it is bridged to. A Layer 3 creates a routed connection where the Lock and User have their own IP networks.

The bridged Key connection allows access only to a specific LAN network and the Locks bridged to it. The routed Key connection allows the selection of multiple LAN networks, Locks and other targets that are accessible for the Key.

Typically, TOSIBOX® edge Node and Key can establish the VPN connection directly between each other using the UDP protocol. There are, however, some cases where this is not possible, for example when outbound UDP is blocked in the firewall, or a proxy server must be used. In these situations, the VPN connection is established using a fallback mechanism using the TCP protocol, with the help of a relay server. The relay server is a Tosibox maintained router on the Internet that re-routes the encrypted VPN data between the connection end points. At no point is the data decrypted at any server because the connections are still end-to-end authenticated and encrypted.

Because of the latencies between the TOSIBOX® products and the relay servers, the nature of the TCP protocol, and server capacity, relayed connections may not provide as good performance as direct UDP connections. To avoid this situation and to ensure the best performance, all outbound UDP connections should be allowed in the firewall.

Remote Connection

TOSIBOX® edge Node and Key identify each other reliably over the Internet because of the matching connection described previously. This unique and patented method by Tosibox creates the connection securely and automatically even through firewalls and NATs. The connection doesn’t require any inbound ports to be permanently open on the firewall. Required outbound ports are listed in the table at the end of this document.

Key - Node connection establishment steps

- Key and edge Node register themselves to the MatchMaker service. The connection between the MatchMaker and TOSIBOX devices is encrypted using TLS and mutually authenticated using certificates and PKI
- User initiates the Key software to request a connection to the edge Node. MatchMaker service listens for connection requests and redirects the connection parameters to the respective end points
- The VPN tunnel is mutually authenticated between the Key software and the edge Node using certificates and PKI
- The VPN tunnel is established directly between the TOSIBOX® edge Node and Key. The connection is end-to-end authenticated and encrypted. Encryption and decryption take place at the connection end points

The only way to access TOSIBOX devices remotely over the Internet is by using the private, secure and encrypted VPN connection that TOSIBOX® creates. Having TOSIBOX® secure connection to the remote site does not cause data security issues to the users or the remote network if the software is kept up to date and access control and system settings are reviewed and maintained systematically.

TOSIBOX® Virtual Central Lock and edge Node configuration UIs are protected from unauthorized users with a username/password. Login is possible only over VPN connection if accessing from the internet or via private LAN side.

Remote access to the network requires Tosibox Key and explicit access rights granted by the network administrator. Tosibox Key provides 2-Factor Authentication, the Key hardware device and a user defined password for login.

Local connection
TOSIBOX® edge Node and user Key can also be used in closed, high security networks to further protect critical systems. In closed networks the TOSIBOX® products connect directly to each other without the need of an internet connection. In addition, connection made outside the network as well as remote connections originating from outside of that closed network can be blocked. This feature is called Local Connection.

Mobile Client
TOSIBOX® Mobile Client for Android and for iOS also adheres to the same high security standards and builds on the physical security foundation of TOSIBOX®. Access rights are granted and controlled from the physical Key device, keeping the Key owner always in control – even if the mobile device would get lost. The Mobile Client utilizes a two-factor authentication scheme where the security credentials are tied to the physical mobile device. The application cannot be copied to or used on another device. Additionally, it is possible to prevent access from Mobile Clients completely per edge Node by the administrator.

Summary
Tosibox is ISO 27001 certified company. With the help of innovative and high-class data security solutions offered by Tosibox, the local network IT administrator can reliably and safely allow remote access onto their LAN.
Some examples of these features:
1. Change user password for the Key software, edge Node and Virtual Central Lock devices
2. Prevent direct internet access from the Key user's computer by activating the Relay users' Internet access mode found in the edge Node menus
3. Audit log data collection and connection monitoring. Audit log collection is implemented on the Virtual Central Lock. VCL collects log data about the events of the VCL itself and also the events of any connected Locks.

TOSIBOX Secure Connectivity Fact Sheet

VPN crypto architecture	PKI with 2048/3072/4096 bit RSA keys, physical or remote key exchange
VPN data encryption	AES 128/192/256 bit CBC, Blowfish
VPN control channel encryption	Managed by VPN library, encryption scheme is negotiated at the beginning of the connection setup, for example AES 256 bit (symmetric AES-256-CBC)
Key Exchange	TLS Diffie-Hellman and client certificates
Matching method (first time)	Physical key exchange or secure remote matching over the internet
Matching method (remotely)	PKI, RSA signed
TOSIBOX® Node and Virtual Central Lock firewall	Yes, Linux iptables
Remote Support from Tosibox	Over SSH, off by default in edge Nodes, on by default in Virtual Central Lock
MatchMaking connection security	TLS/SSL with PKI key exchange and client certificates, data encryption AES 128 bit

Information privacy	Tosibox does NOT require details of customers' devices, private keys or passwords beyond device public IP addresses and device ID's used for providing the networking service
Required open firewall ports	Outbound TCP: 80, 443, 8000, 57051 Outbound UDP: random, 1-65535 Inbound: none
Virtual Central Lock	IP connections from the Internet towards and from Virtual Central Lock must be non-restricted. Virtual Central Lock provides firewalling for securing the network