TOSIBOX Information Security

TOSIBOX® products initiate a remote connection that has a very high level of information security. The encryption and decryption process is always done in the TOSIBOX® products at the end points, e.g. Locks and Keys. The only information transmitted over the Internet is the highly encrypted data sent via the TOSIBOX® units connected between the central location and their remote LANs.

TOSIBOX® products identify each other by cryptographic pairing (matching) in which the products must be matched to each other before use. This is achieved by connecting the TOSIBOX® products together physically. In the matching process, the key device (Key) is inserted into the USB port of the Lock device. The Lock and Key then exchange the public key of the keypair with each other in order to create a mutual trust relationship. The encryption key is stored in a closed memory location of the cryptoprocessor on the Key device. It cannot be copied or tampered with. Establishing a connection is impossible without the correct encryption keys. Additionally, each encrypted data stream is protected with disposable encryption keys that are exchanged with the DH method.

TOSIBOX® Locks and Keys identify each other over the Internet because of the matching connection made as described above. This unique method, patented by Tosibox, creates the connection securely and automatically even through firewalls and NATs. The connection doesn't require any ports to be permanently open on the firewall. TOSIBOX® products 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 requirement of an Internet connection. In addition, connections made outside the network as well as remote connections originating from outside of that closed network can be blocked. This is feature is called 'Offline Mode'.

The only way to access the remote TOSIBOX® Locks is by using the private, secure and encrypted VPN connection that TOSIBOX® creates. When correctly implemented, adding TOSIBOX® remote connections to the LAN does not cause any data security issues to the users of that remote network.

Finally, using the Layer 3 connection type for the remote connection prevents spoofing (forging) of MAC and IP addresses and makes it impossible to flood the network with broadcast traffic.

Tosibox Oy
Teknologiantie 12 A
90590 Oulu, Finland

Sales, Finland tel. +358 44 709 0100
Sales, International tel. +358 44 709 0200

With the help of innovative and high-class data security solutions offered by Tosibox, the local network IT administrator can reliably and safely allow Internet access onto their LAN so that changes can be made to the configuration of the TOSIBOX® Lock. Some examples of these features are shown below:

1. Changing the 'admin' password for the Lock device.
2. Prevent direct Internet access from the Key user´s computer by activating the routing mode found in the 'Industry/Advanced Settings' dialogue of the Lock's set up menus.
3. Extra security can be added by only allowing remote access to designated servers and/or other network appliances by using the IP/MAC filtering function. This too is found in the 'Industry/Advanced Settings' dialogue of the Lock's set up menus.

Tosibox's mobile solution, the Mobile Client for Android and iOS, also adheres to the same high security standards and builds on the physical security foundation of TOSIBOX® products. Firstly, the 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. Secondly, the Mobile Client utilises a two-factor authentication scheme where the security credentials are tied to the physical mobile device. This means that the application cannot be copied to or used on another device. Additionally, in the Lock settings it is possible to prevent access from Mobile Clients completely if the Lock administrator chooses to do so.

TOSIBOX Protection Techniques

VPN crypto architecture	PKI with 2048/3072/4096 bit RSA keys, physical key exchange
VPN data encryption	AES 128/192/256 bit CBC, Blowfish 128 bit CBC
VPN control channel encryption	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® Lock firewall	Yes (Linux netfilter)
Remote Support from Tosibox Oy	Off by default
IP/MAC filtering	Yes
Prevent traffic between TOSIBOX® Keys	Yes
MatchMaking connection security	TLS/SSL with DH key exchange and client certificates, data encryption AES 128 bit
Information privacy	Tosibox Oy does NOT retain any details of customers' devices, private keys or passwords

Additional information: Jari Tenhunen, Tosibox Oy, jari.tenhunen@tosibox.com