TOSIBOX DATA SECURITY

TOSIBOX products initiate a remote connection that has a very high level of data security. The encryption and decryption process is always done inside the TOSIBOX devices, i.e. 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 LAN's.

TOSIBOX devices identify each other by cryptographic pairing (serialization) in which the devices must be serialised/paired with each other before use. This is completed by connecting the TOSIBOX devices together physically. In the serialisation process, the key device (Key) is inserted into the USB port of locking device (Lock). The Lock and Key then exchange the public key of the keypair with each other in order to create a mutual and confidential relationship. The encryption key is stored in a closed memory location of the crypto processor on the Key device. It cannot be copied. Establishing a connection is impossible without the correct encryption keys. Additionally each encrypted data stream is protected by disposable encryption keys exchanged with the DH method.

TOSIBOX Locks and Keys identify each other over the internet because of the serialisation connection made as described above. This unique method, patented by TOSIBOX, creates the connection securely and automatically even through the firewalls. The connection neither needs nor requires ports to be permanently open on the firewall. TOSIBOX devices can also be used in closed high security networks to further protect critical systems. In closed networks the TOSIBOX devices 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 called 'Offline Mode'.

The only way to access the remote TOSIBOX Lock's is using the private, secure and encrypted VPN connection 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 TOSIBOX Layer3 remote connection security feature prevents spoofing (forging) of MAC and IP addresses and makes it impossible to flood the network with broadcast traffic.

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 Settings' dialogue of the Locks set up menus.
3. Extra security can be added by only allowing remote access to designated servers and/or other network appliances by selecting and adding the MAC address filtering function. This too is found in the 'Industry Settings' dialogue of the Locks set up menus.

TOSIBOX protection techniques:

VPN crypto architecture	PKI with 1024 bit RSA keys, physical key exchange
VPN data encryption	Blowfish 128 bit (symmetric BF-128-CBC)
VPN control channel encryption	AES 256 bit (symmetric AES-256-CBC)
Key Exchange	TLS/SSL Diffie-Hellman and client certificate
Serializing method (first time)	Physical key exchange
Serializing method (remotely)	PKI, RSA 1024 bit signed
TOSIBOX Lock firewall	Yes (Linux netfilter)
Remote Support from TOSIBOX Oy	Off by default
MAC filtering	Yes (Mode B)
Prevent traffic between TOSIBOX Keys	Yes
MatchMaking connection security	TLS/SSL with DH key exchange and client certificate, data encryption AES 256 bit (AES-256-CBC)
Information privacy	TOSIBOX Oy does NOT retain any details of customer devices, private keys or passwords

Additional information: Veikko Ylimartimo, TOSIBOX Oy, veikko.ylimartimo@TOSIBOX.com