ZigBee Security

ZigBee security, which is based on a 128-bit AES algorithm, adds to the security model provided by IEEE 802.15.4. ZigBee's security services include methods for key establishment and transport, device management, and frame protection.

The ZigBee specification defines security for the MAC, NWK and APS layers. Security for applications is typically provided through Application Profiles.

Trust center

The Trust Center decides whether to allow or disallow new devices into its network.

The Trust Center may periodically update and switch to a new Network Key. It first broadcasts the new key encrypted with the old Network Key. Later, it tells all devices to switch to the new key.

The Trust Center is usually the network coordinator, but is also able to be a dedicated device. It is responsible for the following security roles:

- Trust Manager, to authenticate devices that request to join the network
- Network Manager, to maintain and distribute network keys
- Configuration Manager, to enable end-to-end security between devices

Security keys

ZigBee uses three types of keys to manage security: Master, Network and Link.

Master keys

These optional keys are not used to encrypt frames. Instead, they are used as an initial shared secret between two devices when they perform the Key Establishment Procedure (SKKE) to generate Link Keys.

Keys that originate from the Trust Center are called Trust Center Master Keys, while all other keys are called Application Layer Master Keys.

Network keys

These keys perform security Network Layer security on a ZigBee network. All devices on a ZigBee network share the same key.
High Security Network Keys must always be sent encrypted over the air, while Standard Security Network Keys can be sent either encrypted or unencrypted. Note that High Security is supported only for ZigBee PRO.

Link keys

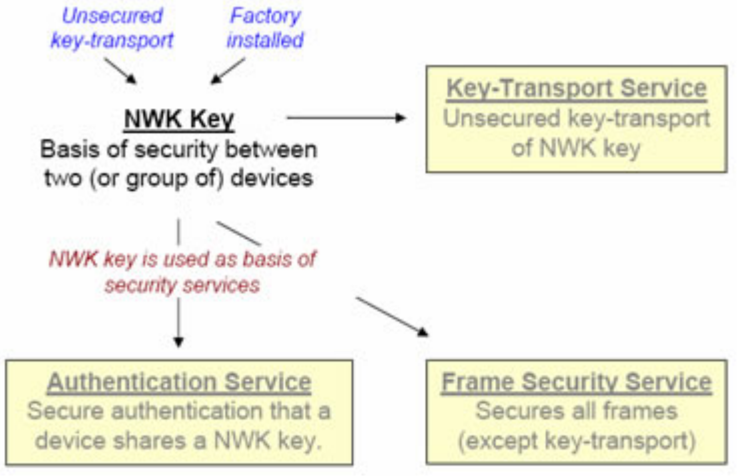
These optional keys secure unicast messages between two devices at the Application Layer.
Keys that originate from the Trust Center are called Trust Center Link Keys, while all other keys are called Application Layer Link Keys.

Security modes

ZigBee PRO offers two different security modes: Standard and High.

Feature	Standard*	High
Network Layer security provided using Network key	✓	✓
APS layer security provided using Link keys**	✓	✓
Centralized control and update of keys	✓	✓
Ability to switch from active to secondary keys	✓	✓
Ability to derive Link keys between devices		✓
Entity authentication and permissions table supported		✓

* Called "Residential" in ZigBee 2006 ** Not supported in ZigBee 2006


Unsecured key-transport
Factory installed
NWK Key
Basis of security between two (or group of) devices
Key-Transport Service
Unsecured key-transport of NWK key
NWK key is used as basis of security services
Authentication Service
Secure authentication that a device shares a NWK key.
Frame Security Service
Secures all frames (except key-transport)

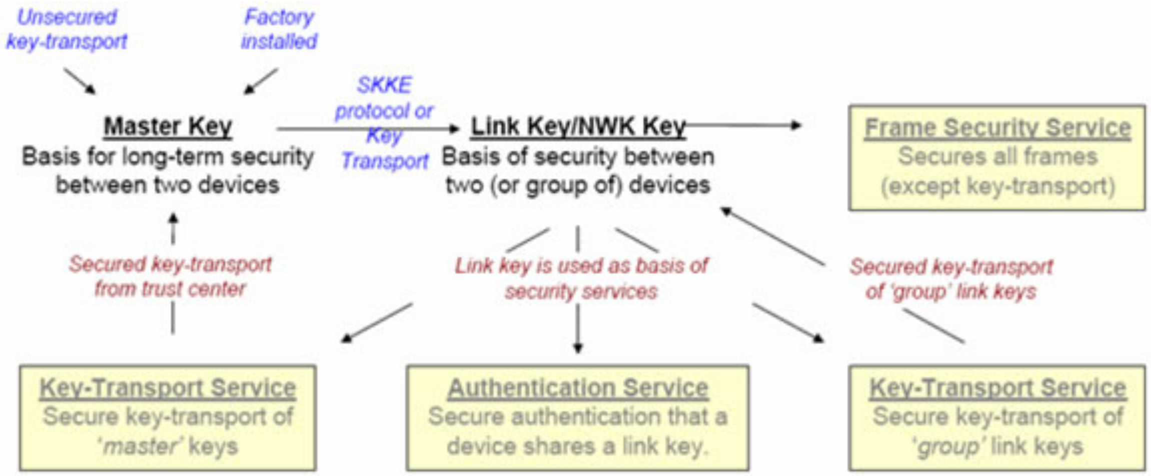
Standard security mode

In Standard Security mode, the list of devices, master keys, link keys and network keys can be maintained by either the Trust Center or by the devices themselves. The Trust Center is still responsible for maintaining a standard network key and it controls policies of network admittance. In this mode, the memory requirements for the Trust Center are far less than they are for High Security mode.

High security mode

In High Security mode, the Trust Center maintains a list of devices, master keys, link keys and network keys that it needs to control and enforce the policies of network key updates and network admittance. As the number of devices in the network grows, so too does the memory required for the Trust Center.

The additional security capabilities inherent in ZigBee PRO are critical as ZigBee is used in increasingly important applications. The control of critical systems infrastructure, whether in a commercial building, utility grid, industrial plant, or a home security system must not be compromised.


Unsecured key-transport
Factory installed
SKKE protocol or Key Transport
Master Key
Basis for long-term security between two devices
Link Key/NWK Key
Basis of security between two (or group of) devices
Frame Security Service
Secures all frames (except key-transport)
Secured key-transport from trust center
Link key is used as basis of security services
Secured key-transport of 'group' link keys
Key-Transport Service
Secure key-transport of 'master' keys
Authentication Service
Secure authentication that a device shares a link key.
Key-Transport Service
Secure key-transport of 'group' link keys