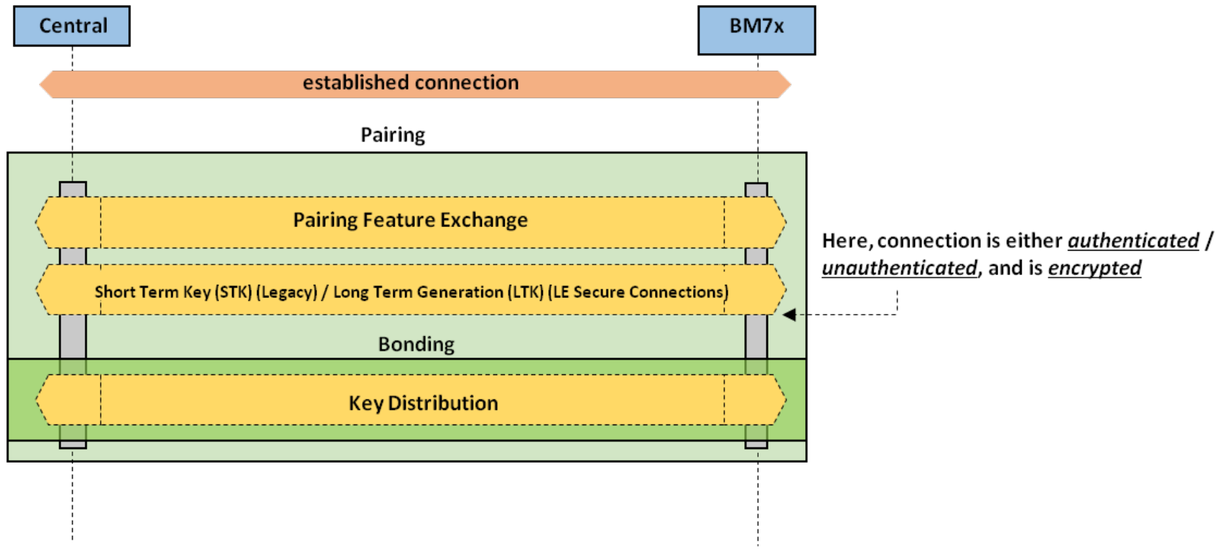
Search This Site
Search
Home
Training
Development Tools
Functions
Embedded Software Integration
Wi-Fi® and Ethernet
Universal Serial Bus
Wired Communications
Wireless Communications
Get Started Here
Bluetooth® Low Energy (BLE)
Fundamentals
Introduction
Architecture
Controller Layer
Host Layer
Generic Access Profile (GAP)
Overview
Roles
Modes & Procedures
Security
Generic Attribute Profile (GATT)
BLE Development on Android Tutorial
LoRa®
Touch Sensing
Motor Control
Power Conversion
Signal Conditioning
Digital Signal Processing
Machine Learning
Authentication

triggered, for example, by a central device that is attempting to access a data value (a "characteristic") on a peripheral device that requires authenticated access. Pairing involves authenticating the identity of two devices, encrypting the link using a Short-Term Key (STKs), and then distributing Long-Term Keys (LTKs) (for faster reconnection in the future, i.e., bonding) used for encryption, as shown:



The new security level of the connection is based on the method of pairing performed and this is selected based on the I/O capabilities of each device. The security level of any subsequent reconnections is based on the level achieved during the initial pairing.

The role each device plays is defined in the Security Manager (SM) portion of the BLE stack. They are:

- Initiator: Always corresponds to the Link Layer Master and therefore the GAP central.
- Responder: Always corresponds to the Link Layer Slave and therefore the GAP peripheral.

Security Modes/Levels of a Connection