Hello, and welcome to this presentation of the features of the STM32WB’s Bluetooth Low Energy peripheral.
The Bluetooth Low Energy (BLE) peripheral handles all real-time operations of the Bluetooth Smart system, controls the Bluetooth Low Energy physical layer (PHY), and Bluetooth Low Energy security. Communication with the Cortex-M4 processor, which handles the Bluetooth Low Energy profiles and application, is done via a memory-mapped mailbox and the Inter Processor Communication Controller.

The BLE peripheral operates autonomously and doesn’t require application Cortex-M4 involvement to maintain a Bluetooth Low Energy connection, perform scanning or advertising, thus enabling an ultra-low-power implementation.

Sharing system and security peripherals is handled via the Hardware Semaphores (HSEM).
The STM32WB supports the main Bluetooth Smart features. A BLE device is either a master or a slave device for one link. The STM32WB supports 8 BLE links simultaneously with a minimum of 2 slaves. The terms Master and Slave are the link layer roles equivalent to Central & Peripheral. The Client Server architecture is done at the GATT (Generic Attribute Profile) layer and used to transfer values.
The STM32WB Bluetooth Low Energy architecture separates the Bluetooth Low Energy Profiles and Application, running on the application Cortex-M4, from the Bluetooth Low Energy real-time aspects residing in the Bluetooth Low Energy peripheral. The Bluetooth Low Energy peripheral incorporates a Cortex-M0+ processor containing the Bluetooth Low Energy STACK handling the link layer up to the Generic Attribute Profile (GATT) and Generic Access Profile (GAP) layers. It also incorporates the Physical 2.4 GHz radio. For more information on the 2.4 GHz radio see the specific RF training.
Communication between the Cortex-M4 and the Bluetooth Low Energy peripheral takes place over a memory-mapped mailbox and the Inter Processor Communication Controller (IPCC) using a Host Controller Interface (HCI) like protocol format to support Application Control Interface (ACI) commands, responses and user events. Different sets of commands, responses, and events are used depending on the final application.
A set of commands supports Generic Access Profiles (GAP) to define the BLE link role. Another set of commands is used for the Generic Attributes Profiles (GATT) to support the transfer of values via the Client Server architecture. Certain vendor-specific commands are used to manage CM0+, CM4 and BLE IP configurations.

- IR is the identity root key used to derive the LTK and CSRK keys,
- ER is the encryption root key used to derive the LTK and CSRK keys,
- DIV is used to derive the CSRK key.
The Bluetooth Low Energy Radio test mode verifies the STM32WB transmit and receive performance. Standard and vendor-specific Host Controller Interface commands are used to place the device in the different test modes. This way, the device can be tested using a Bluetooth tester or with a PC and RF measurement equipment.
The Bluetooth Low Energy peripheral autonomously controls the system’s low-power Sleep, Stop, and Standby modes based on the Bluetooth Low Energy operating modes. When waking up from low-power modes, the Bluetooth Low Energy peripheral detects the system’s operating mode and autonomously configures its system clock to ensure the application Cortex-M4 state remains unchanged. The sharing of the Power Controller and Reset & Clock controller resources with the Cortex-M4 is managed via hardware semaphore, preventing any blocking of resource sharing.
Some security peripherals are securable by the Cortex-M0+, to grant exclusive access to the Bluetooth Low Energy peripheral. The AES2, PKA and True RNG functions can be fully secured for use by the Bluetooth Low Energy peripheral. The AES1 cryptographic keys can be secured so that secure keys can be used to encrypt data by the application Cortex-M4. These peripherals allow sharing on a needed basis between the Cortex-M4 and the Bluetooth Low Energy peripheral. The use of shared peripherals is managed via the hardware semaphore IP (HSEM). For application cryptography, the Bluetooth Low Energy peripheral provides secure key management with features to store, update, delete and load keys.
To guarantee correct real-time operation of the Radio system during critical radio phases, low-latency access is granted to the Flash memory. During this phase, it is not possible to initiate new “erase” and “store” Flash operations. The Cortex-M4 can obtain real-time radio system information using the radio critical phase flag and interrupt.
Each Bluetooth device is allocated a unique 48-bit device address, which is a 48-bit extended unique identifier (EUI-48) created in compliance with the IEEE 802-2014 Universal addresses standard. The STM32WB provides a 64-bit unique device identifier based on the 24-bit ST company ID, an 8-bit Dory device ID, and a 32-bit unique number. This STM32WB 64-bit unique device identifier can be used to derive the unique Bluetooth 48-bit device address, avoiding having to program the unique identifier in production.
Here is an overview of the peripheral’s status at specific low-power configuration modes. The BLE peripheral can operate in all low-power Sleep, Stop, and Standby modes, except forShutdown mode. The BLE peripheral is capable of autonomously waking up from any low-power mode without the need for the Cortex-M4. When needed, the BLE peripheral interrupts and wakes up the Cortex-M4 from CRun, CSleep, and CStop modes.
In addition to this training, you may find the Flash Memory Interface and System Configuration trainings useful.