Democratizing the Establishment of Secure Connections

Donnie Garcia
Solutions Architect, NXP Semiconductors

MARCH 3, 2020

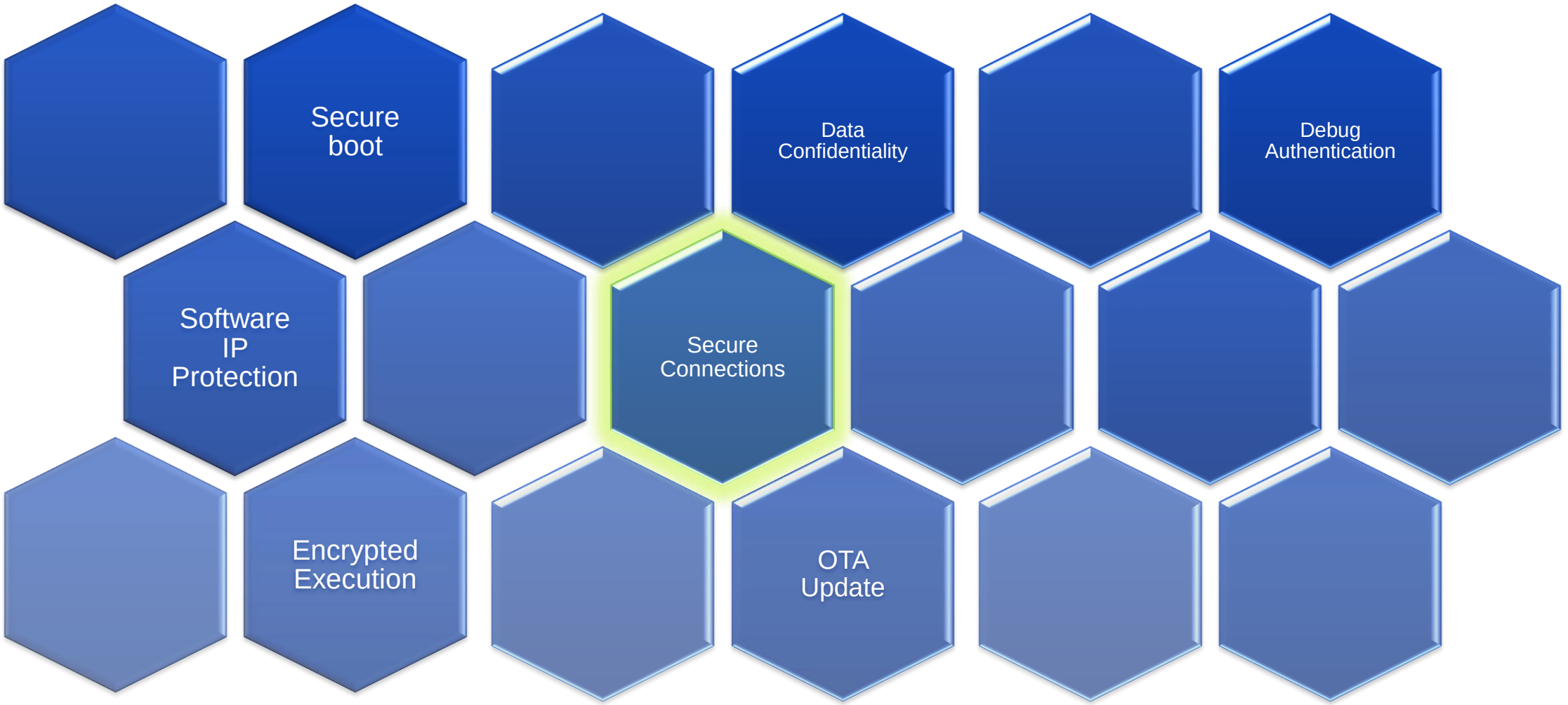
SECURE CONNECTIONS FOR A SMARTER WORLD

OUR EMBEDDED WORLD

SENSE	THINK	CONNECT	ACT
			
EVERYTHING	EVERYTHING	EVERYTHING	EVERYTHING
Aware	Smart	Connected	Efficient

EVERYTHING SAFE & SECURE

EXPLORING EMBEDDED CYBERSECURITY



NEAR FIELD COMMUNICATIONS (NFC)

- NFC is a contactless short range technology, based on inductive coupling (10cm / 4 in)
- Co-invented in 2002 by NXP and Sony
- Operating frequency 13.56MHz, speed < 848 kbits/s

Big reasons to consider NFC

More Intuitive
It's like shaking hands

Power Efficient
Only one of the two devices needs to be powered

Trusted Addition for other Technology
Especially for pairing devices

NFC USE CASES ARE GROWING

Identification & Authentication
of consumables and accessories to help combat counterfeits or configure the main unit based on accessory

Parameterization & Diagnosis
using a phone as an extended user interface for small, sealed and unpowered devices

Pair with Bluetooth & WiFi
devices faster, without conflicts with just a tap of your phone

Access Control
Use your phone or smart card to open doors or give access to machine configurations

SIMPLE SECURE PAIRING WITH A SINGLE TAP

Pair your phone faster with Bluetooth devices, without conflicts

Tap your WiFi router to get an instant WiFi connection

Pair wireless accessories to your main unit

NFC Benefits

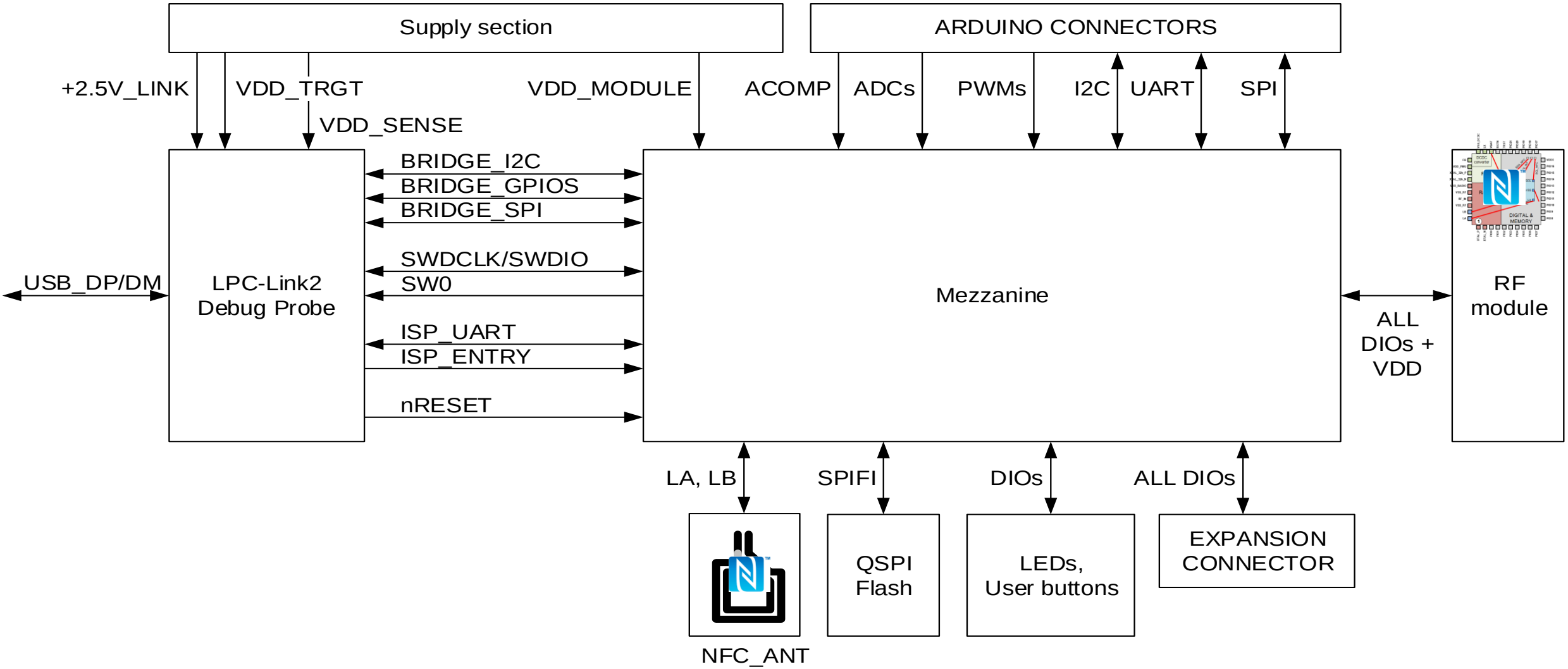
- Pair devices 20x faster than with BLE or WiFi
- Identify a device instantly (no device conflicts or codes)
- Make devices easier to use
- Reduce tech-support costs
- Ensure that accessories are paired to the correct device

THE LATEST IN CONNECTED INTELLIGENCE: QN9090/30 (T)

High Capability and Low Power Bluetooth® 5 SoC with Built-in NFC Option

The QN9090 and QN9030 are the latest devices in the QN series of Bluetooth low energy devices that achieve ultra-low-power consumption and integrate an Arm® Cortex®-M4 CPU with a comprehensive mix of analog and digital peripherals. These highly capable devices allow developers to create products that have rich features and address ease of use with optional NFC technology.

DESIGN KIT CARRIER BOARD HIGH LEVEL BLOCK DIAGRAM

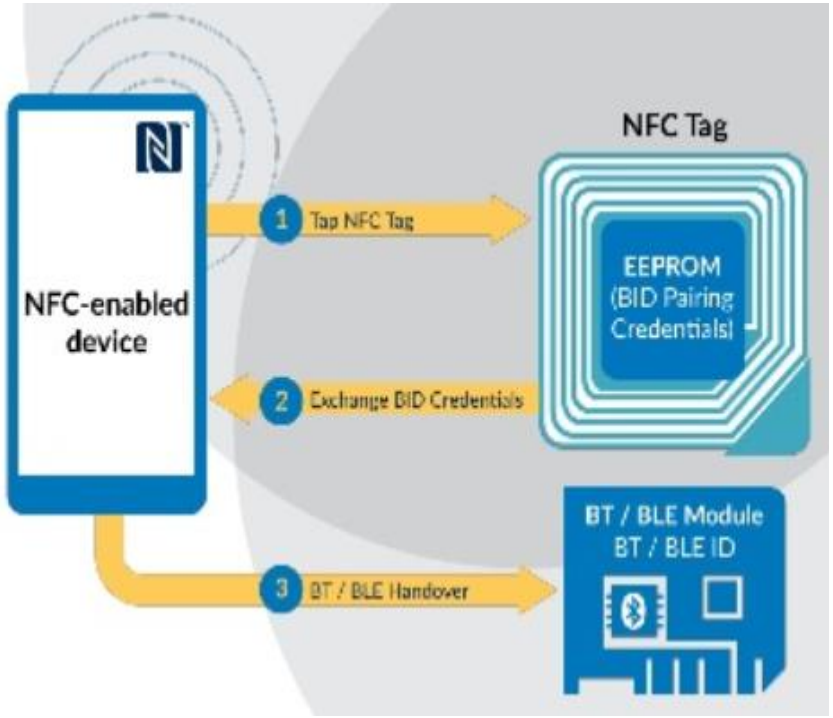


CONNECTION HANDOVER

- Defined by NFC Forum
- Data transaction handed over to other carrier(Bluetooth, Wifi, etc) from NFC to improve communication distance or throughput.
- Enhance user experience
  - Select device directly without discovery procedure, no need scanning
  - Connect to a Bluetooth device fast and securely, authenticating by NFC link
  - Start specific application based on NFC record

BLE OOB PAIRING IMPLEMENTATION – HANDOVER

- **Negotiated Handover**
  - Adopted on the device equipped with NFC Forum Device supporting **peer-to-peer mode**
  - Have transaction of Handover Request Message and Handover Select Message
  - Choice of the carrier embodied in the message
- **Static Handover**
  - Adopted on the device equipped with NFC Forum Tag
  - Stored Handover Select Message in tag
  - Handover Selector Device detects the message and reads it from tag
  - Choice of the carrier embodied in the message
- **Simplified Tag Format**
  - Adopted on the device equipped with NFC Forum Tag
  - Does not use Handover Select record
  - Contains an NDEF message with only the Bluetooth OOB information



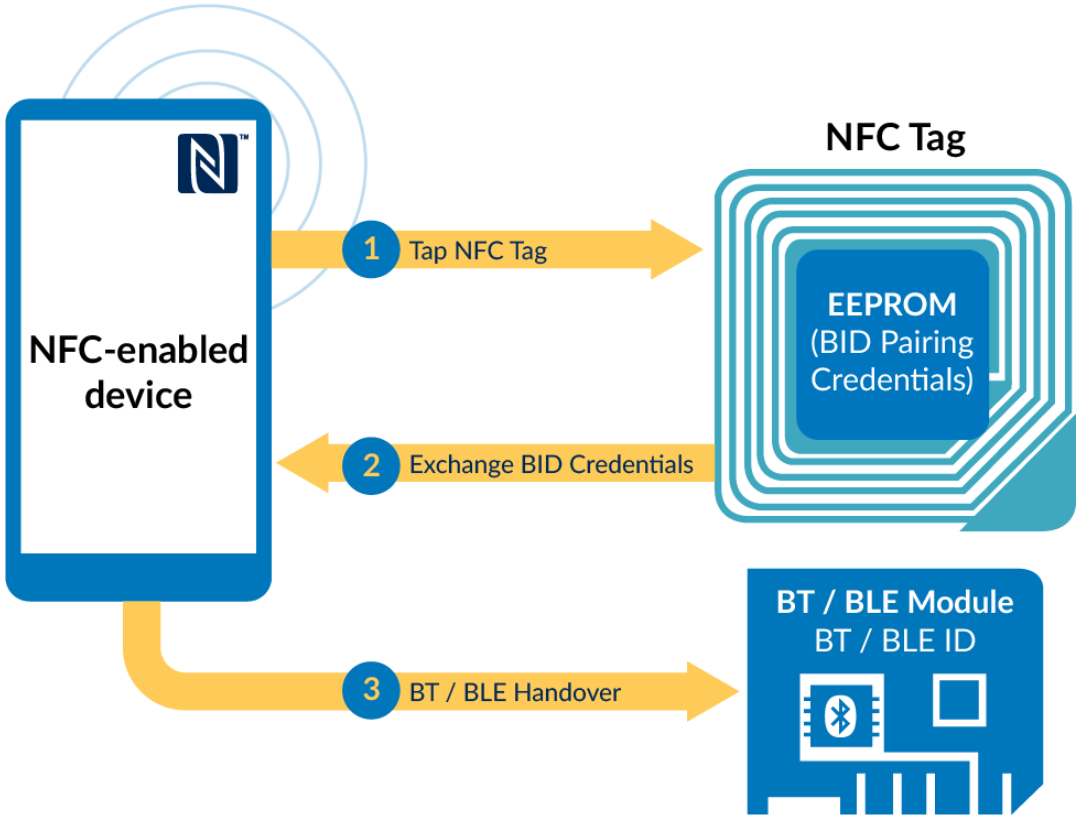
BLE OOB PAIRING IMPLEMENTATION – OOB DATA

Type	Value(1 Octet)	Description
Mandatory	0x1B	LE Bluetooth Device Address
	0x1C	LE Role
Optional	0x10	Security Manager TK Value
	0x19	Appearance
	0x01	Flags
	0x08 or 0x09	Local Name

BLUETOOTH SECURE PAIRING WITH NFC

Easy Bluetooth pairing process

- Tap the NFC tag
- Exchange Pairing Credentials
- Handover to BT / BLE



HELPFUL RESOURCES

- QN9090
  - https://www.nxp.com/products/wireless/bluetooth-low-energy/qn9090-30t-bluetooth-low-energy-mcu-with-armcortex-m4-cpu-energy-efficiency-analog-and-digital-peripherals-and-nfc-tag-option:QN9090-30

- NFC
  - https://www.nxp.com/products/rfid-nfc/nfc-hf/ntag/nfc-tags-for-electronics:MC_1429877262080

SECURE CONNECTIONS
FOR A SMARTER WORLD