MT7688 Secure Gateway & Module Reference Design

Content

- Project Information
- Introduction
  - MT7688 Secure Module
  - MT7688 IoT Gateway
- Security
- PCB Information
- Sub-Systems

Project Information

Objectives

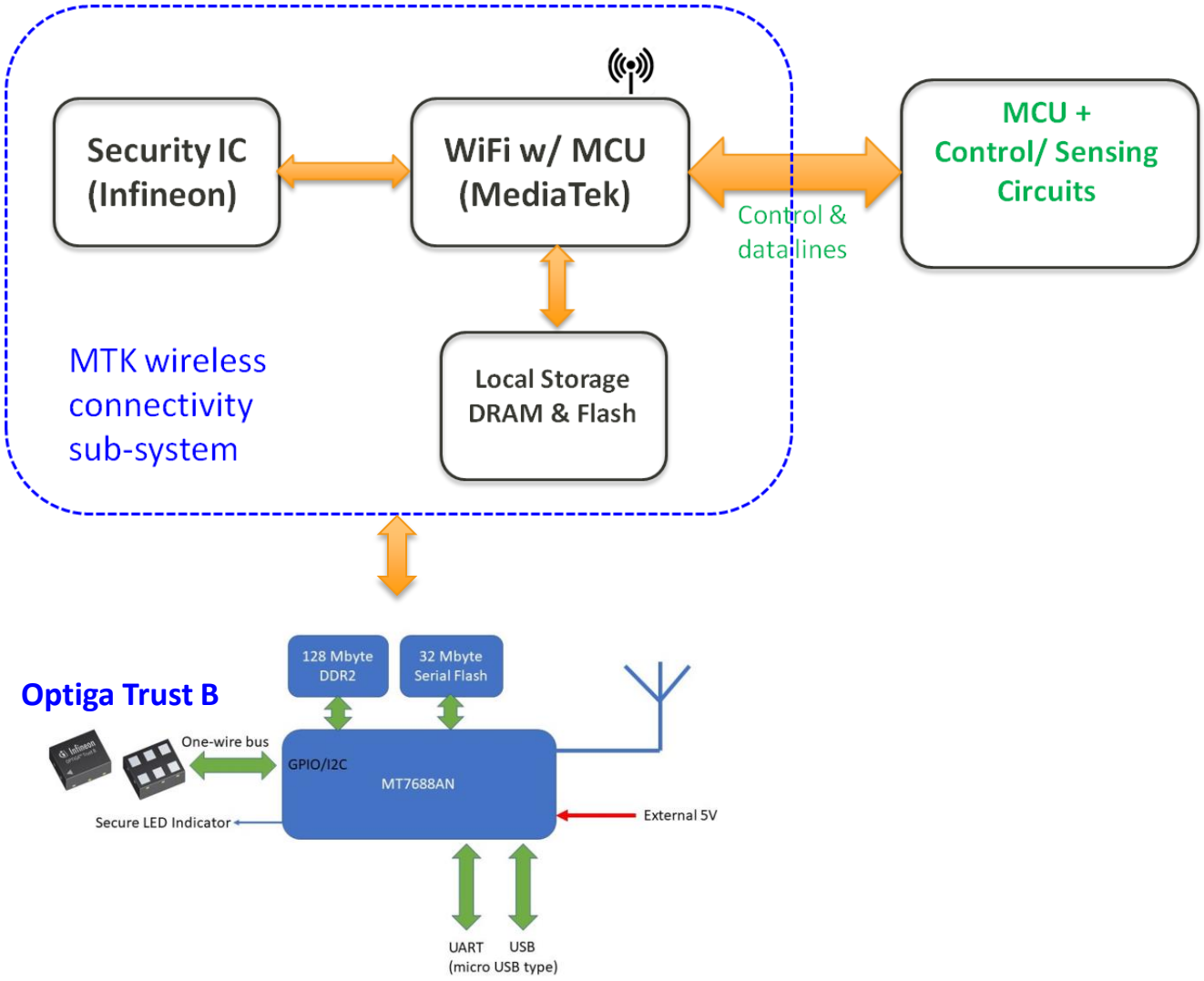
- To develop an IoT solution with hardware security features.
- The solution includes gateway and module using MT7688.
- Two securities IC will be included in this platform:
  - IoT gateway – TPM 1.2 (SLB 9645)
  - IoT edge device – Optiga Trust-B (SLE95250)
- Demo set and module will be developed.

Design Approach

- One PCB to support two Infineon security products: TPM 1.2/2.0 & Optiga Trust B.
- MT7688 is a master chip for both setup. It interfaces with the security IC and perform 2.4GHz Wi-Fi connectivity functions.
- Dual-board approach is adopted.
  - Module board: MT7688 + Optiga Trust B + DRAM + Flash
  - Base board: TPM + other connectivities

Wi-Fi Module
&
IoT Gateway

MT7688 Module for IoT Edge Devices

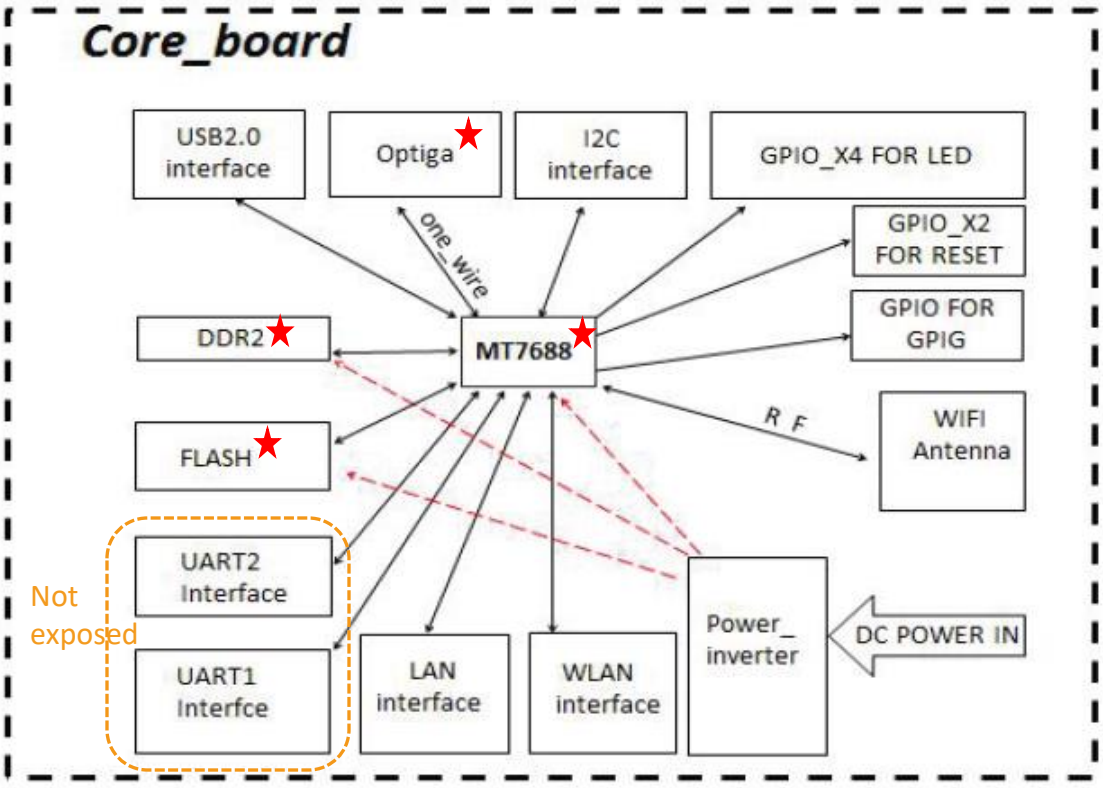


Features of MT7688 Secure Module

- Applications:
  - Interface with sensors or IoT edge devices
- The module includes:
  - MT7688AN (WiFi 802.11b/g/n & MIPS CPU (580MHz))
  - Serial Flash (64/32 Mbyte)
  - DDR RAM (128 Mbyte)
  - Infineon Security Optiga Trust B (SLE95250)
  - Crystal 40MHz
  - 6-layer PCB (34mm x 20mm)
  - Antenna ipex connector
  - Other discrete parts
  - Able to switch among gateway, AP and repeater mode

Functional Blocks of MT7688 Module

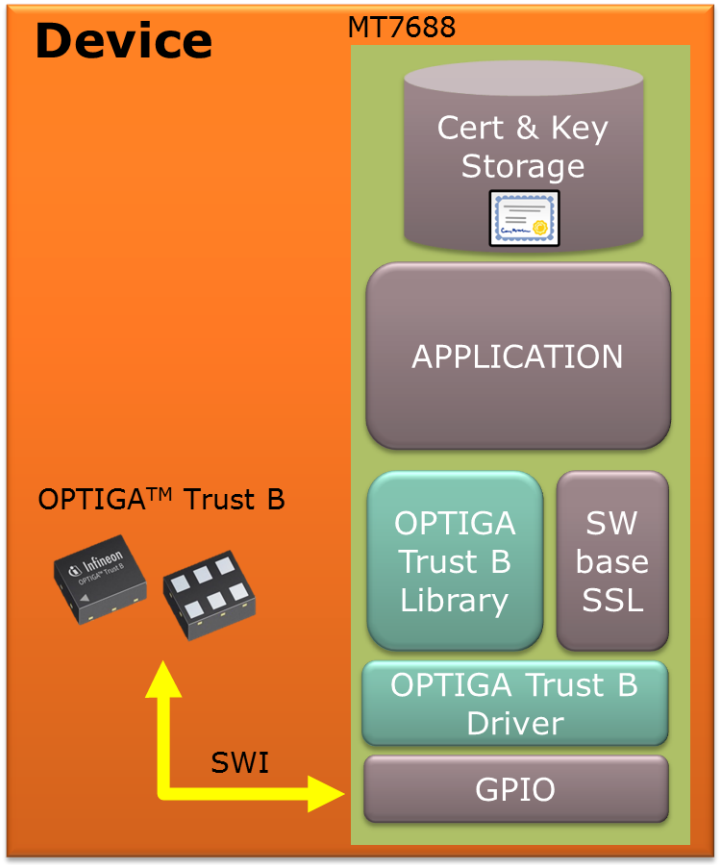
- Core board:



Advantages of MT7688 Secure Module

- For IoT edge device with MT7688 and Optiga Trust B:

1. Each node has unique hardware identity (96 bits UID) that can be used in device management on the Server
2. To deter hardware cloning with the use of ECC based ODC and challenge-response mechanism implementation
3. Secret Key used for challenge and response is stored in tamper resistant hardware and never leave the hardware
4. Service/brand protection as each customer will have unique ODC public key
5. Support Enhanced system security by integrating the ODC into the standard X.509 certificate



Security for IoT Edge Device

- How device security (Trust B) and registration work? Need Infineon input

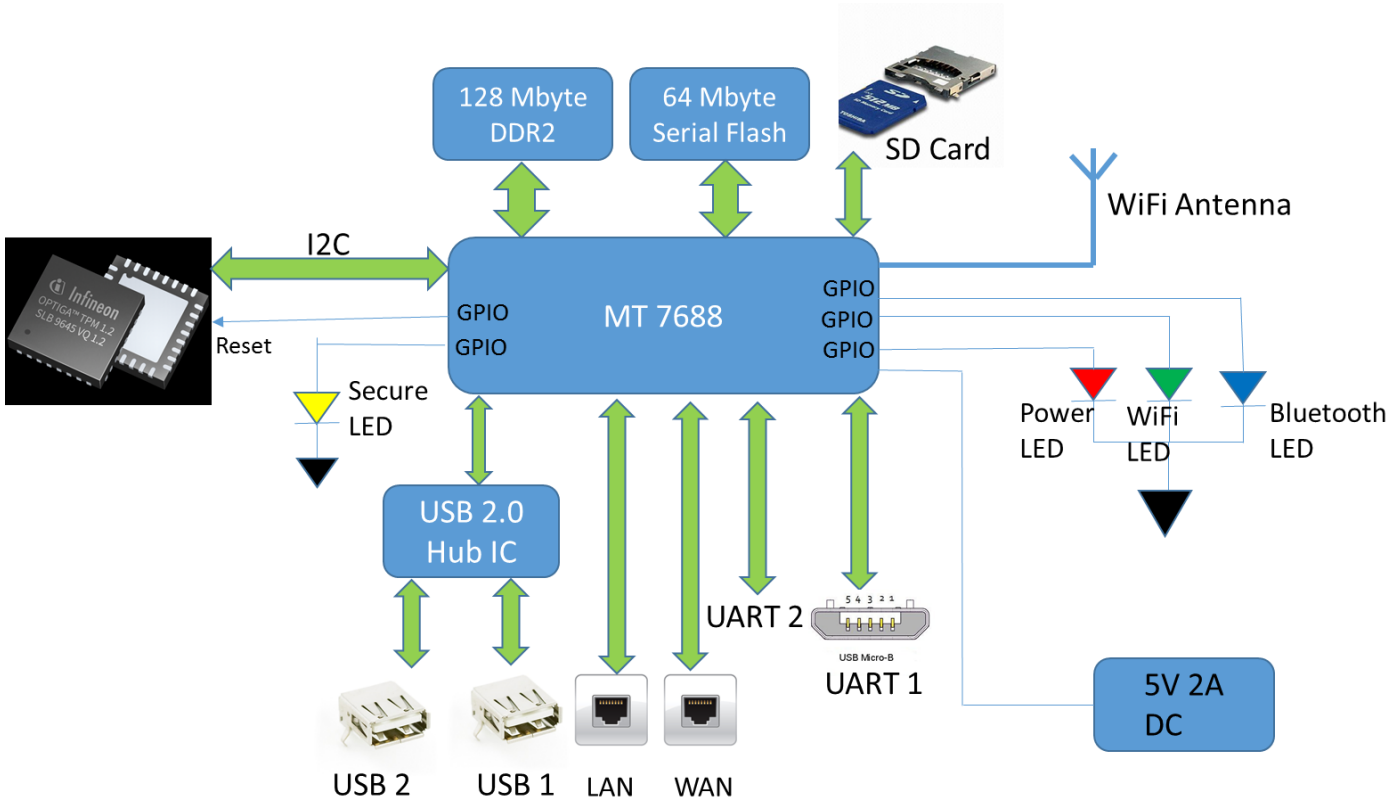
MT7688 Secured Module

MT7688 module

Dimension (W x H):
20mm x 33.6mm

IoT Gateway Reference Design

- MT7688 + TPM 1.2

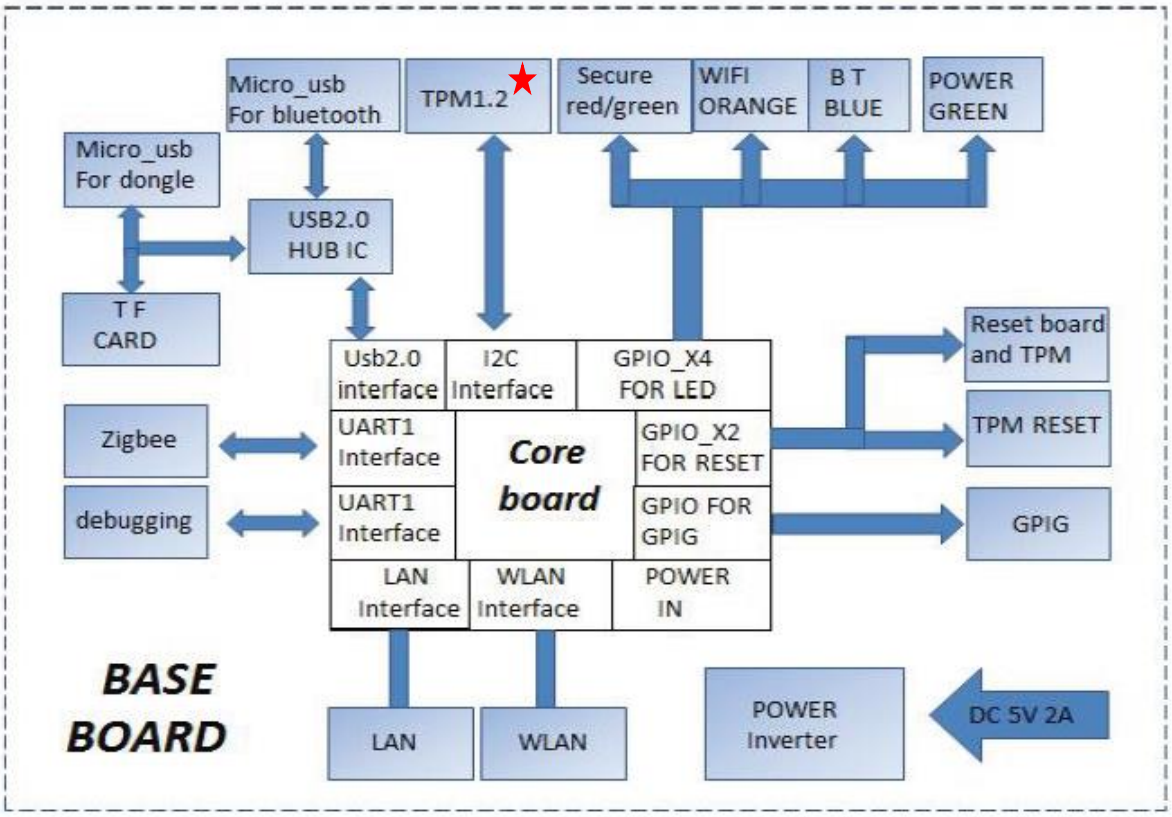


Features of Gateway

- Applications:
  - Gateway to manage and control IoT edge devices.
  - Modular design where the core module can independently be configured as node
- The gateway provides the following features and connectivity:
  - Wi-Fi IEEE 802.11b/g/n, 2.4GHz
  - Authentication via TPM 1.2 or 2.0
  - Serial Flash (64 Mbyte)
  - DDR RAM (128 Mbyte)
  - 1x WAN port: RJ45 Connector, 10/100Mbps
  - 1x LAN port: RJ45 Connector, 10/100Mbps
  - 2x USB ports: For connecting to other USB devices, e.g. LTE/3G, ZigBee or Bluetooth dongle
  - 1x TF Card Slot
  - 1x Micro USB
  - 2 Buttons: 1 for system reboot or WiFi reset; 1 for TPM physical presence
  - 4 LED Light to display status (RED/GREEN/ORANGE/BLUE).

Functional Block of Gateway

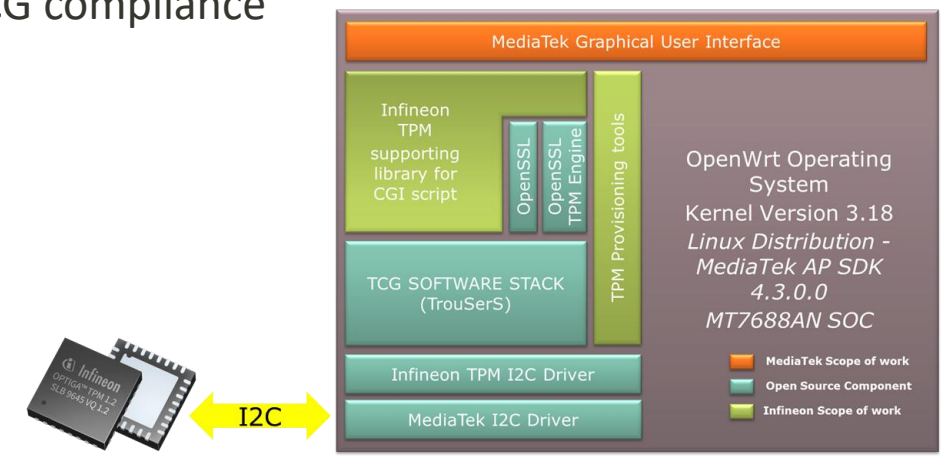
- Base board:



Advantages of MT7688 Secure Gateway

- For MT7688 IoT Gateway with TPM:

1. Authentication via TPM protected X.509 certificate for SSL/TLS transport security
2. OPTIGA TPM protects important credential with access right control mechanism
3. Keys are always generated by the TPM and private keys never leave TPM in plain text
4. Secure storage and access of keys, passwords and certificates
5. Dictionary attack lock-out feature effectively deters malware that repeatedly guessing system passwords
6. Support platform integrity measurement feature with the use of PCRs
7. Support remote attestation implementation by server
8. Interoperable due to TCG compliance



Security for IoT Gateway

- How device security (TPM) and registration work (IoT edge device and remote cloud server)? Need Infineon input

Secured Gateway for IoT Applications

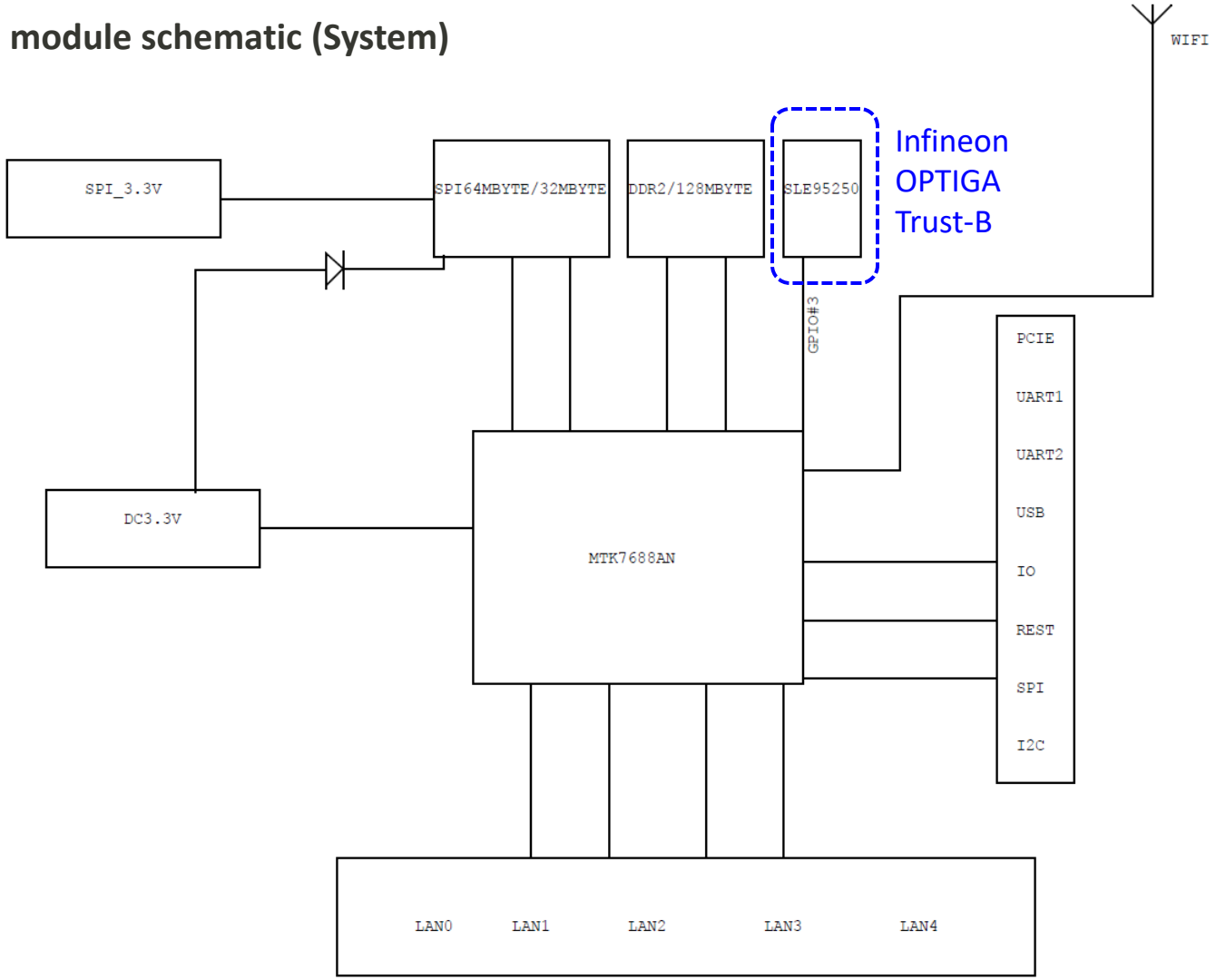
MT7688 module

Gateway base board with
connectivity & TPM

PCB Information

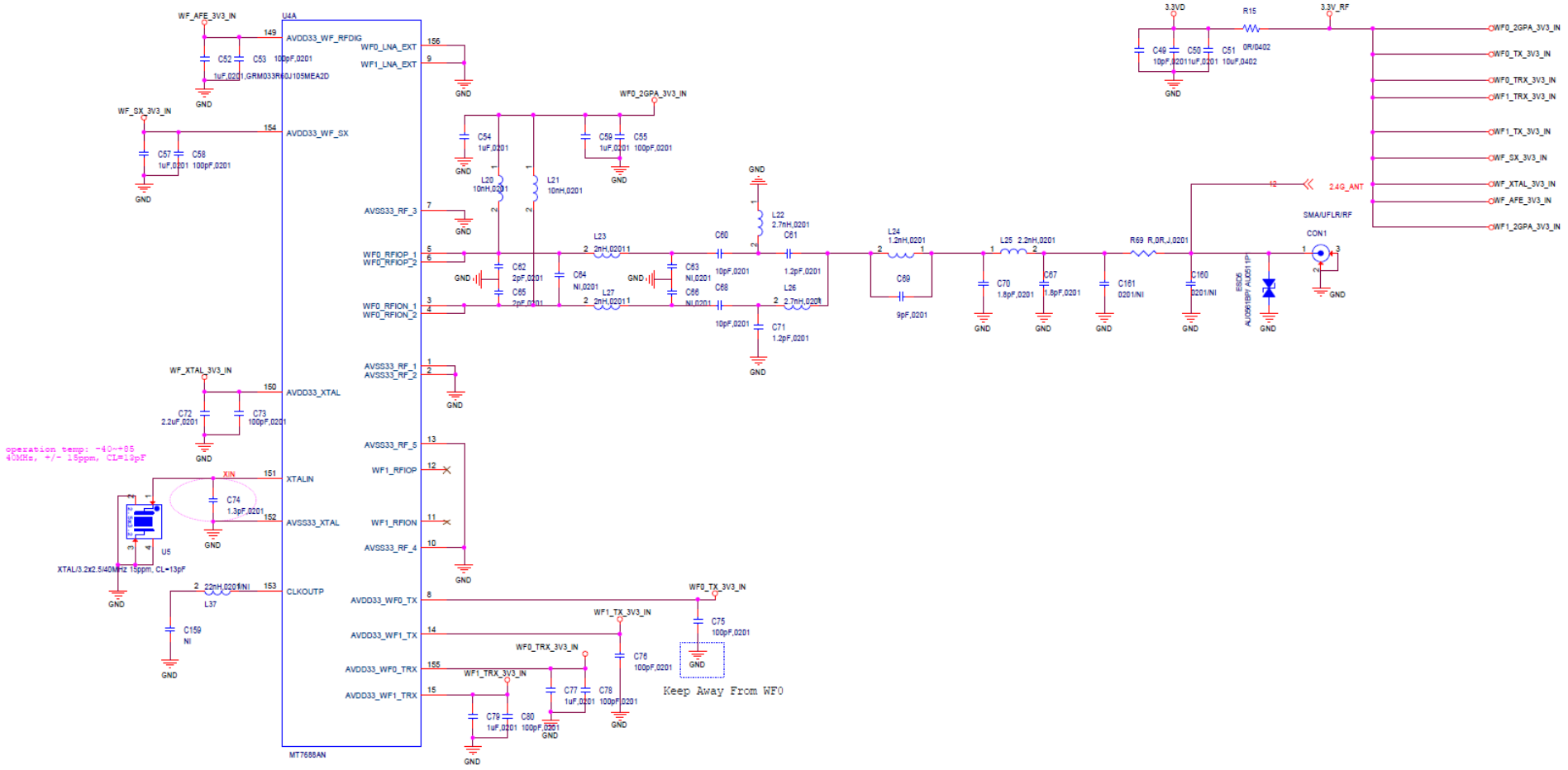
MT7688 Module PCB

MT7688 module schematic (System)



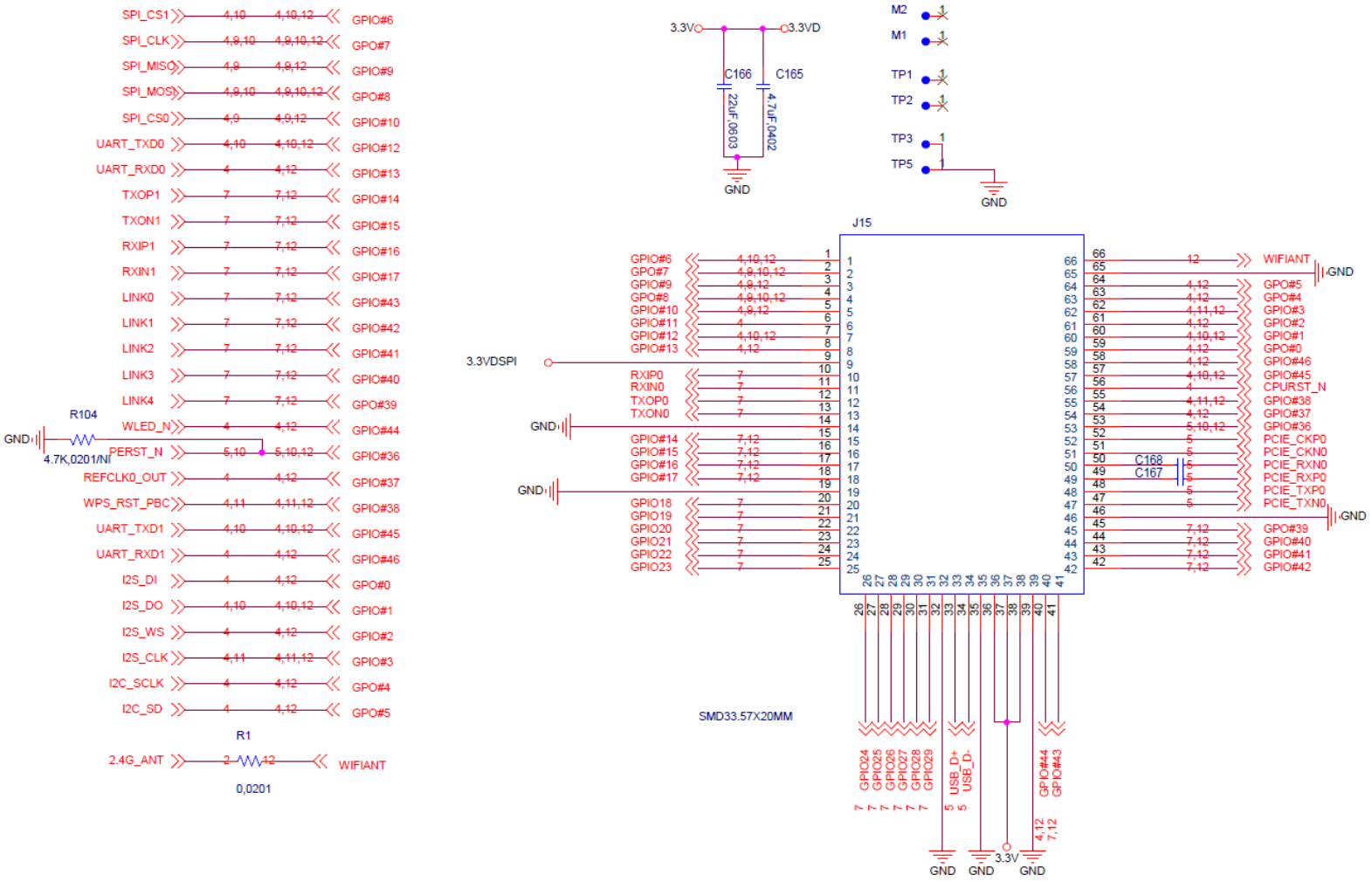
MT7688 Module PCB

MT7688 module schematic (RF and input matching network)



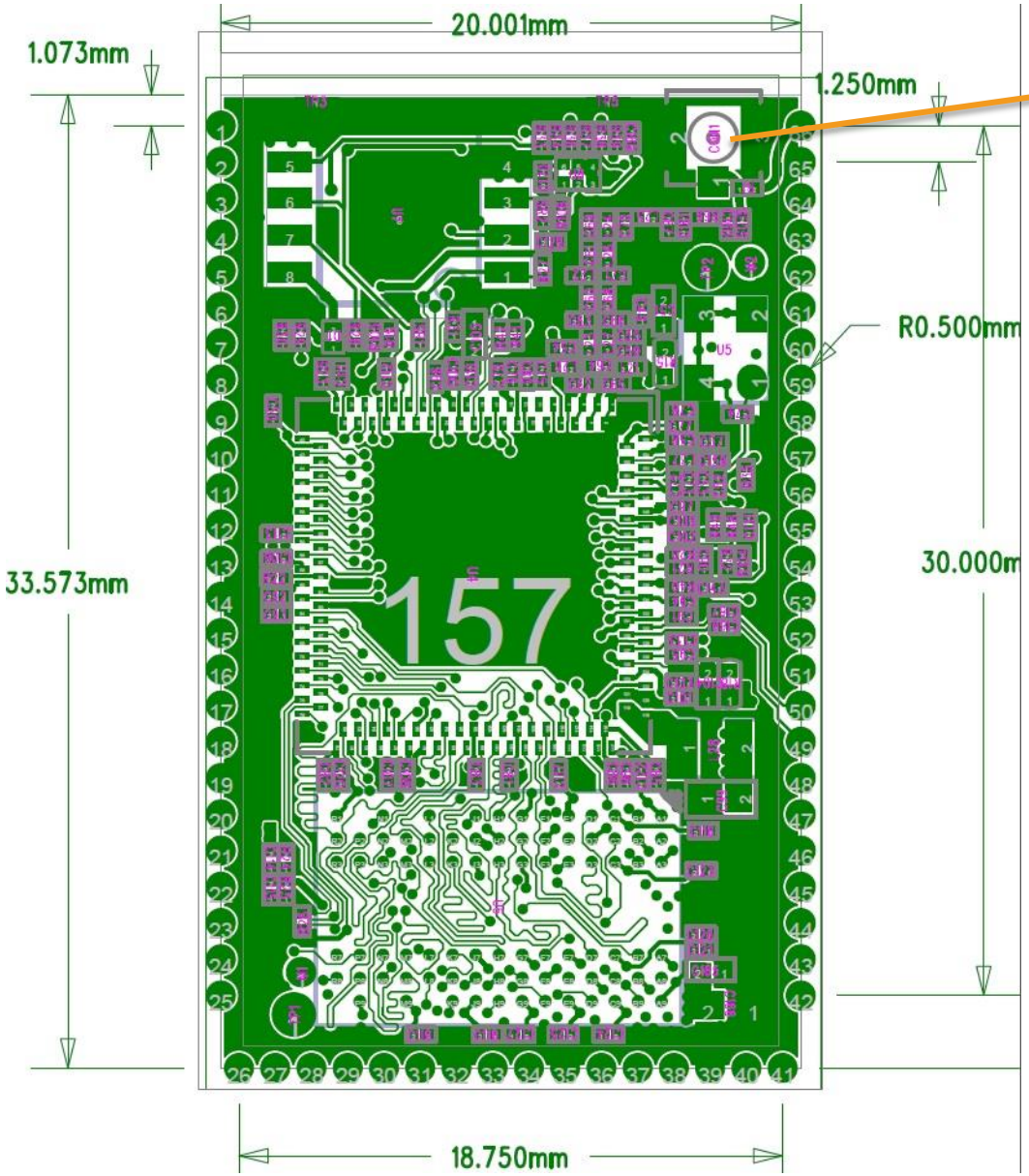
MT7688 Module PCB

MT7688 module schematic (GPIOs)



MT7688 Module PCB

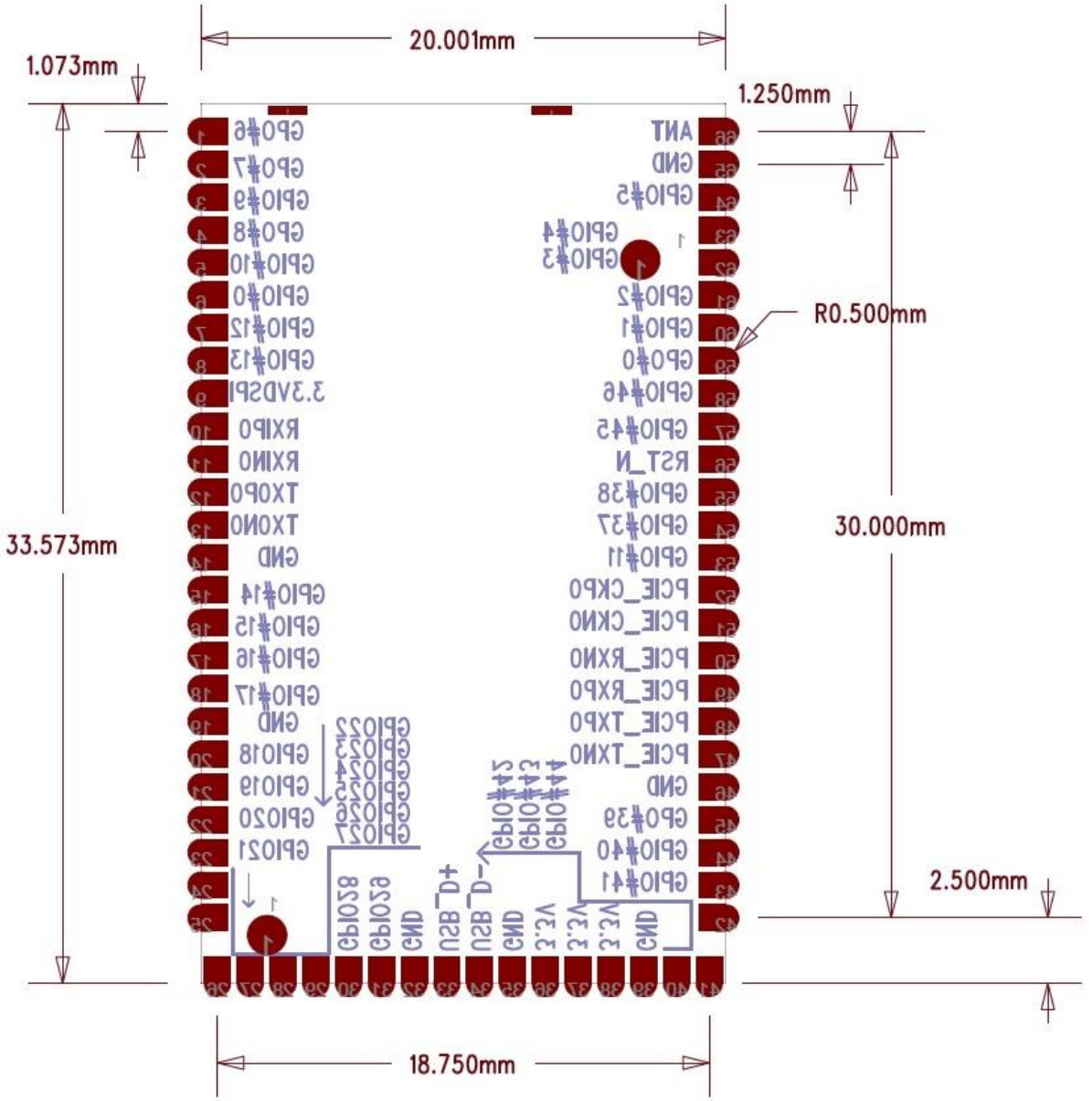
MT7688 module PCB Layout



External IPX antenna

MT7688 Module PCB

MT7688 module I/O



MT7688 Module PCB

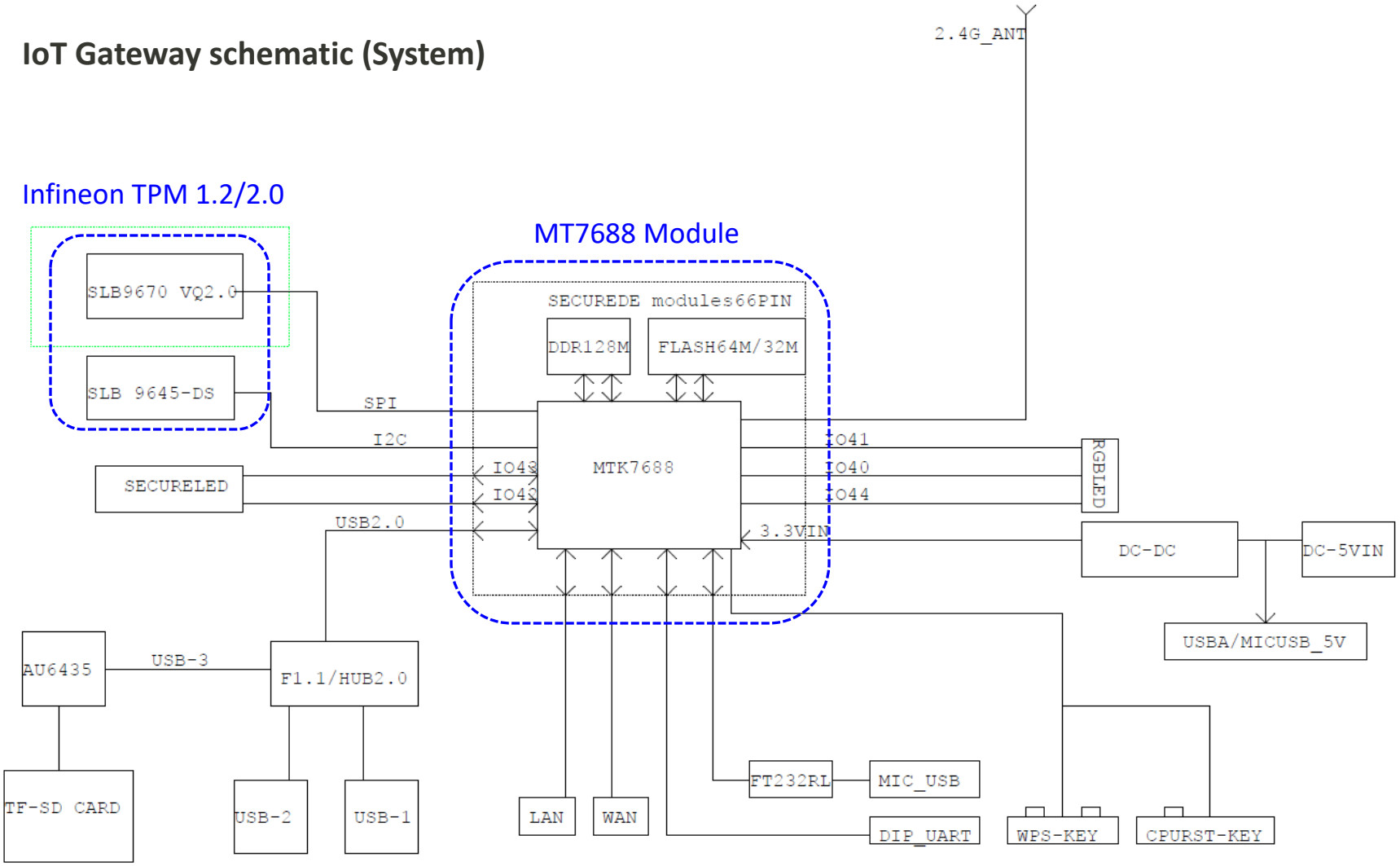
MT7688 module Pin Assignments

	MTK (IOT)	MTK (GW)				MTK (GW)	MTK (IOT)
		SPI_CS1	GPO# 6	1	66	ANT	
		SPI_CLK	GPO# 7	2	65	GND	
		SPI_MISO	GPIO#9	3	64	GPIO#5	I2C SLB9670/SLB9645
		SPI_MOSI	GPO#8	4	63	GPIO#4	I2C SLB9670/SLB9645
		SPI_CS0	GPIO#10	5	62	GPIO#3	TrustB Reset
		GPIO#11	GPIO0	6	61	GPIO#2	TPM_RESET
		UART0	GPIO#12	7	60	GPIO#1	TPM_ForceCleaer
		UART0	GPIO#13	8	59	GPO#0	
			3.3VDSPI	9	58	GPIO#46	UART1
	Port0	Port0	RXIP0	10	57	GPIO#45	UART1
			RXIN0	11	56	RST_N	CPURST_N(SW3硬复位)
			TX0P0	12	55	GPIO#38	WPS(SW4)
			TX0N0	13	54	GPIO#37	GPIO#37
			GND	14	53	GPIO#36	PERST_N
	GPIO#14/eMMC	Port1	GPIO#14	15	52	PCIE_CKP0	PCIE_CKP0
	GPIO#15/eMMC		GPIO#15	16	51	PCIE_CKN0	PCIE_CKN0
	GPIO#16/eMMC		GPIO#16	17	50	PCIE_RXN0	PCIE_RXN0
	GPIO#17/eMMC		GPIO#17	18	49	PCIE_RXP0	PCIE_RXP0
			GND	19	48	PCIE_TXP0	PCIE_TXP0
	GPIO#18/eMMC	Port2	GPIO#18	20	47	PCIE_TXN0	PCIE_TXN0
	GPIO#19/eMMC		GPIO#19	21	46	GND	
	GPIO#20/eMMC		GPIO#20	22	45	GPO#39	P4_LED_AN
	GPIO#21/eMMC		GPIO#21	23	44	GPIO#40	BT LED
	GPIO#22/eMMC	Port3	GPIO#22	24	43	GPIO#41	POWER GREEN LED
	GPIO#23/eMMC		GPIO#23	25	42	GPIO#42	SECURE GREEN LED

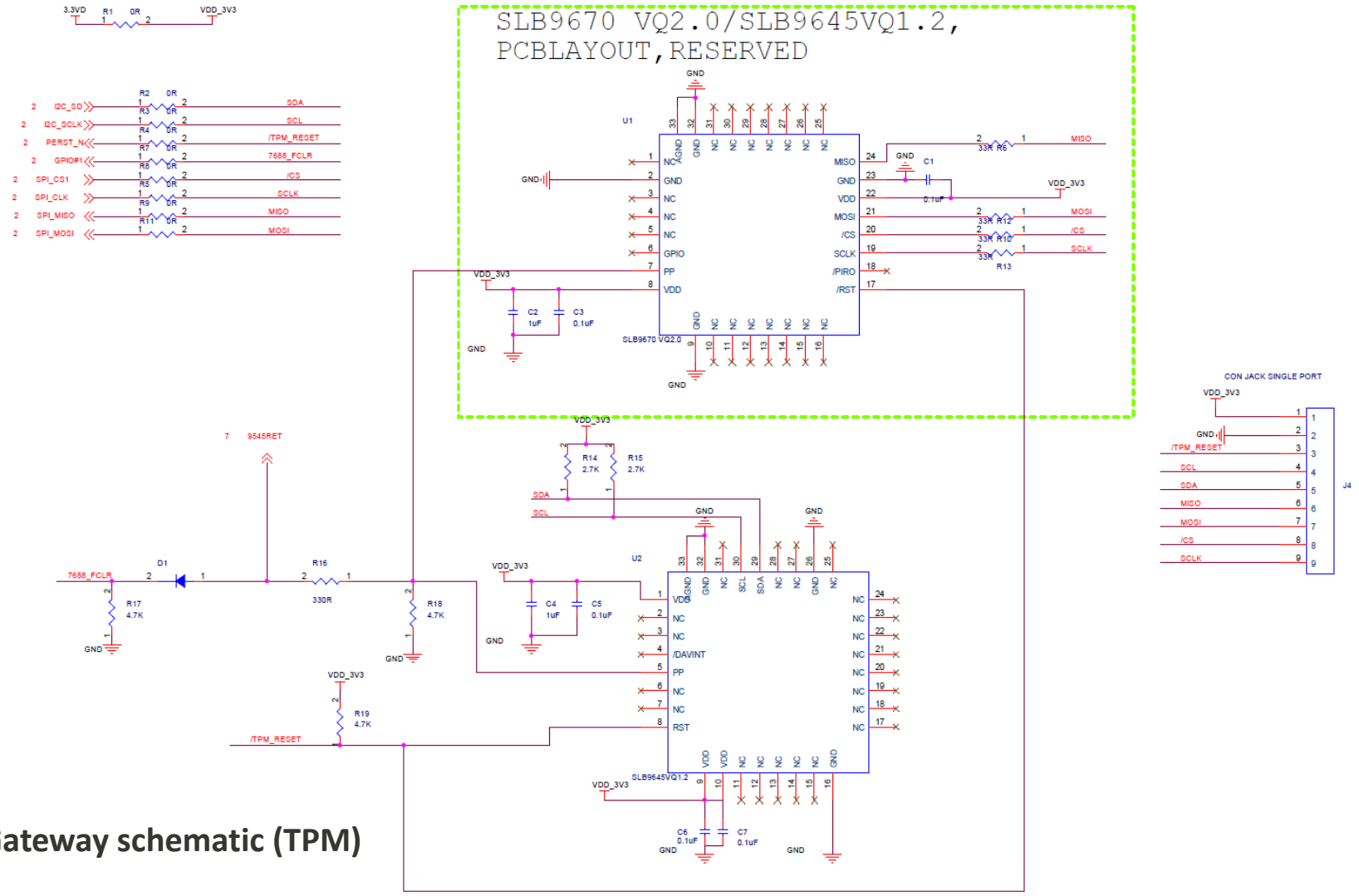
	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
	GPIO#24	GPIO#25	GPIO#26	GPIO#27	GPIO#28	GPIO#29	GND	USB_D+	USB_D-	GND	3.3V	3.3V	3.3V	GND	GPIO#44	GPIO#43
MTK (GW)	Port3		Port4												WiFi Orange LED	SECURE RED LED
MTK (IOT)	GPIO#24/eMMC	GPIO#25/eMMC	GPIO#26/eMMC	GPIO#27/eMMC	GPIO#28/eMMC	GPIO#29/eMMC										

IoT Gateway Base PCB

IoT Gateway schematic (System)

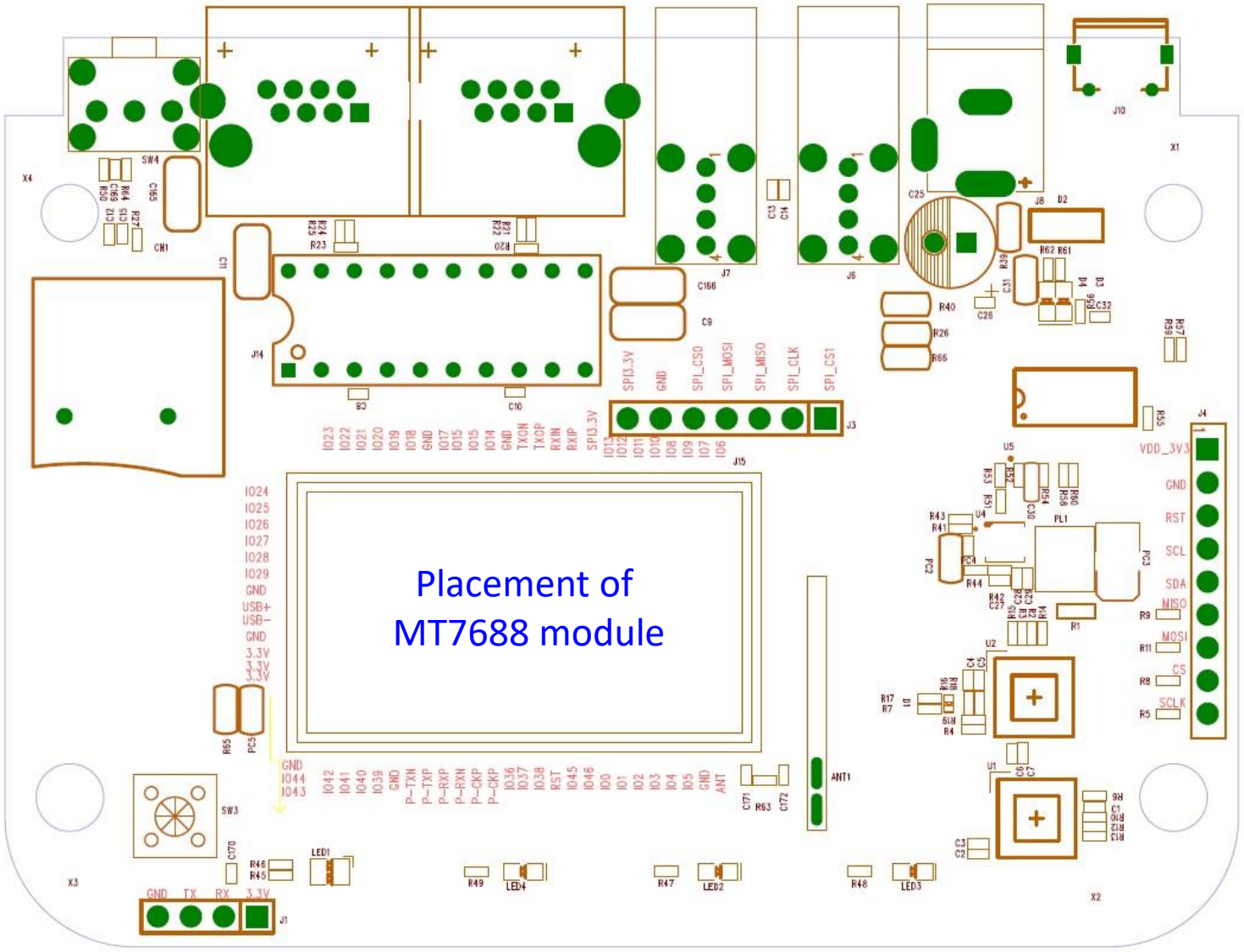


IoT Gateway Base PCB

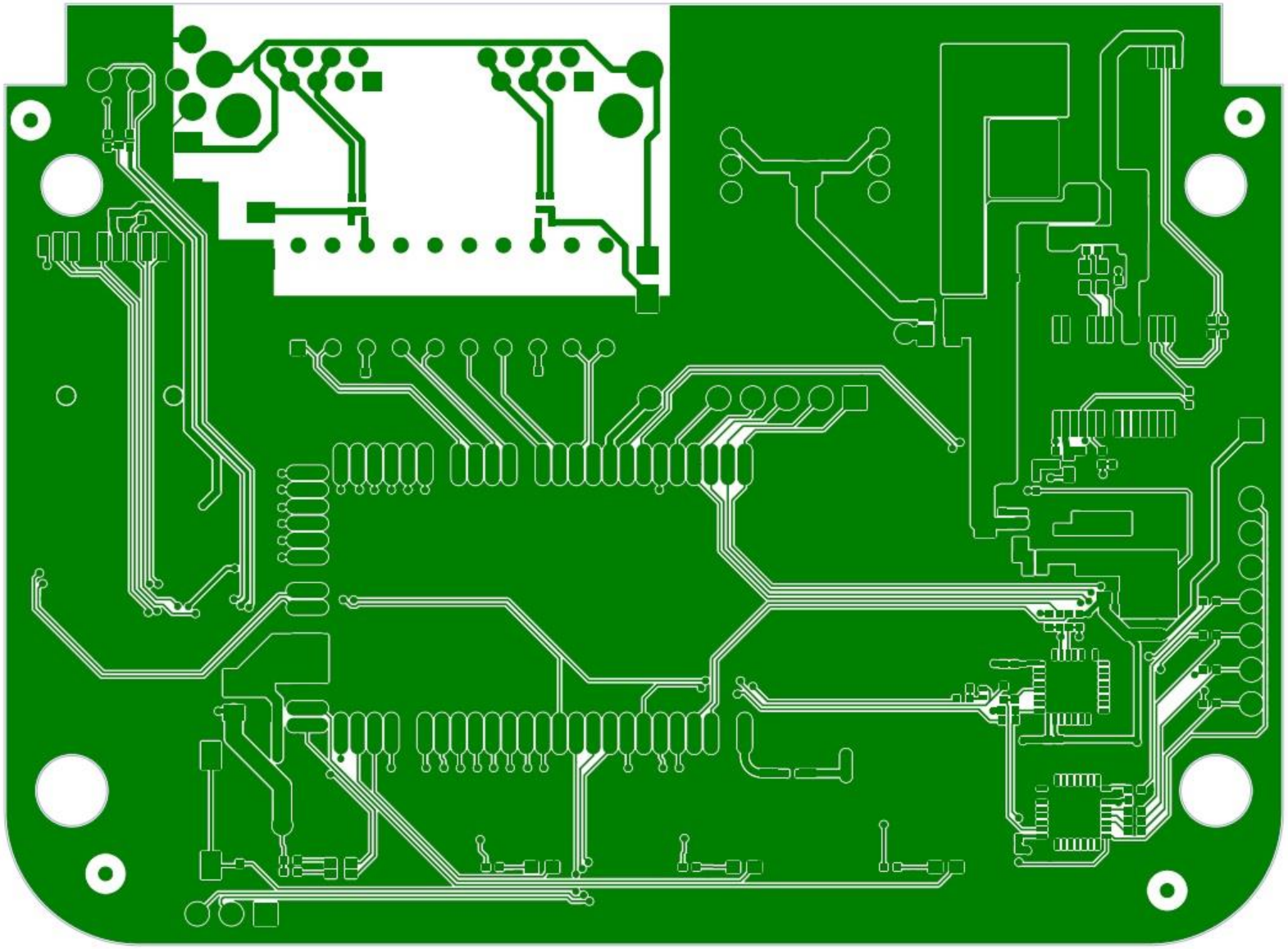


IoT Gateway schematic (TPM)

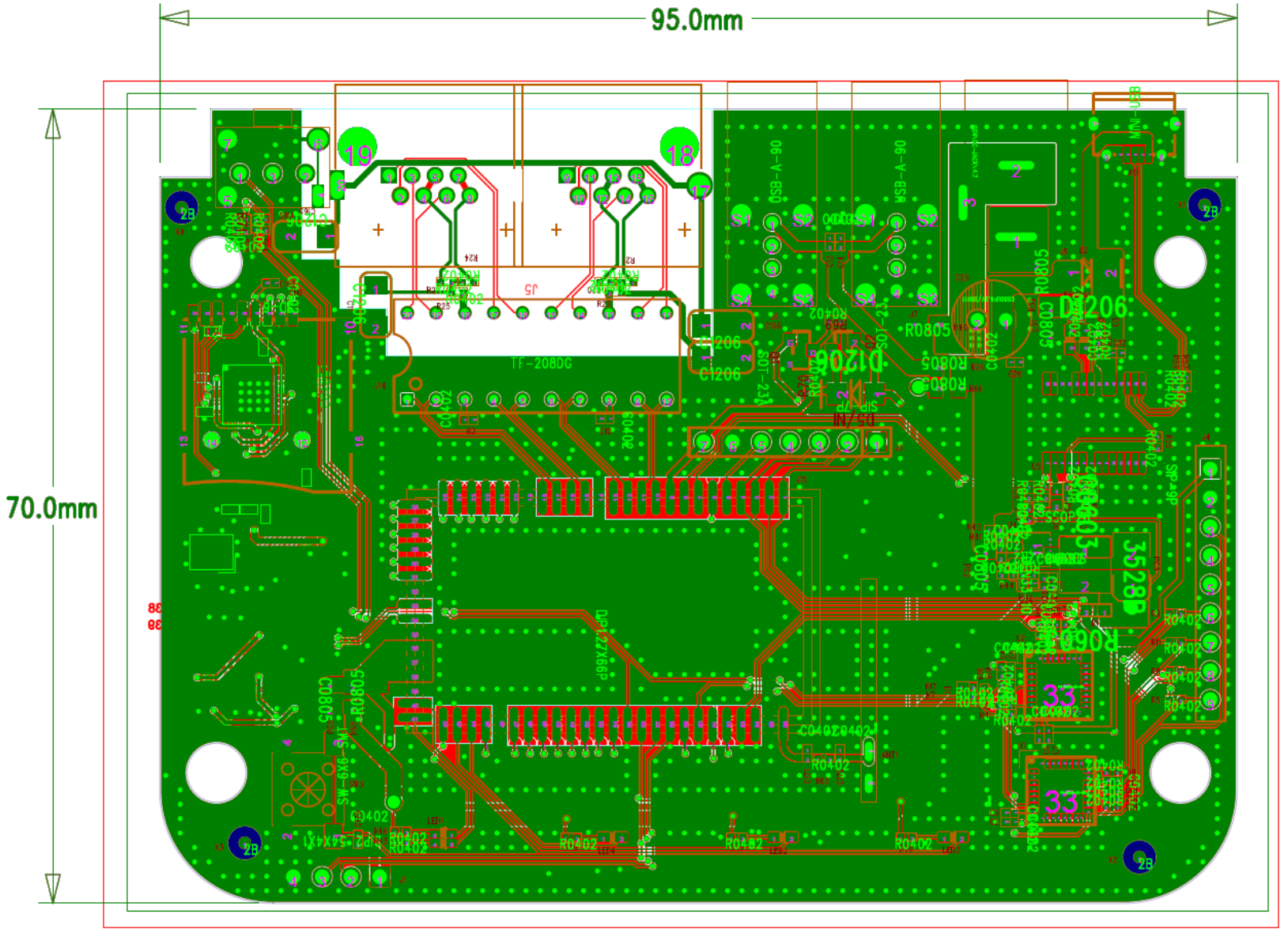
IoT Gateway Base PCB



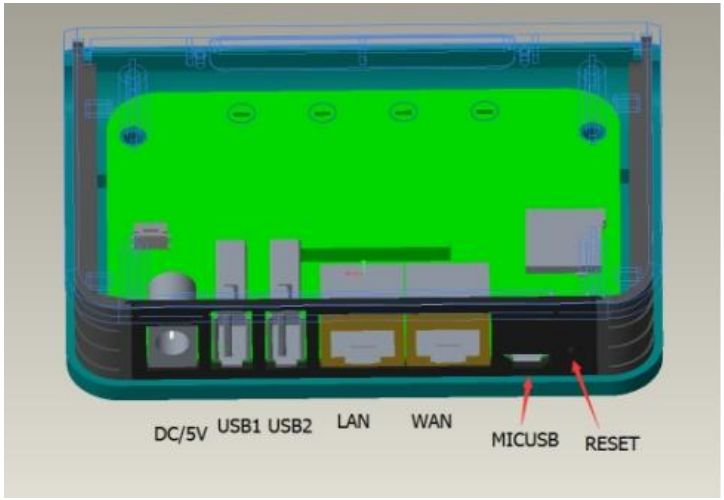
IoT Gateway Base PCB

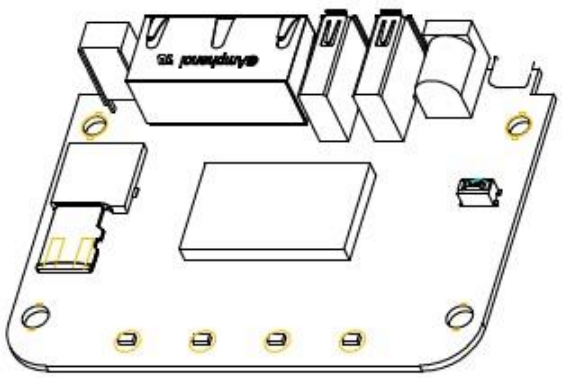


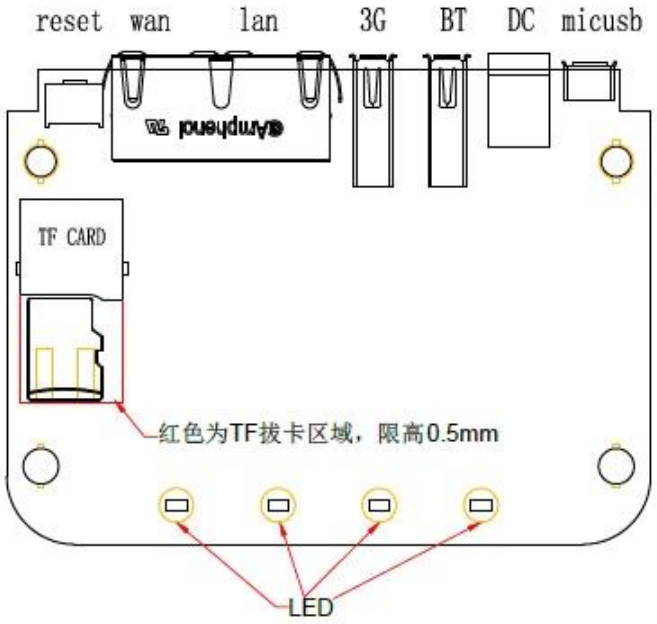
IoT Gateway Base PCB

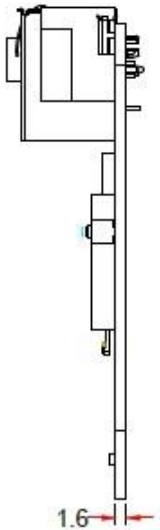


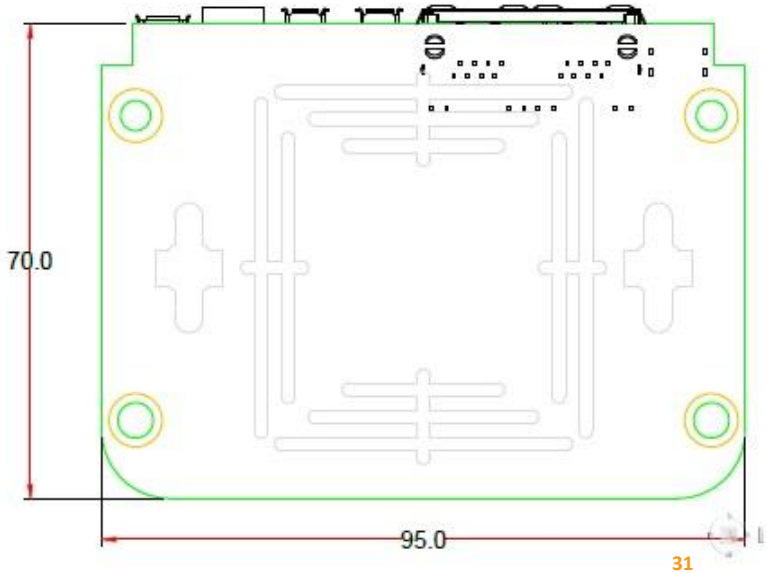
Gateway PCB Mechanical Drawing







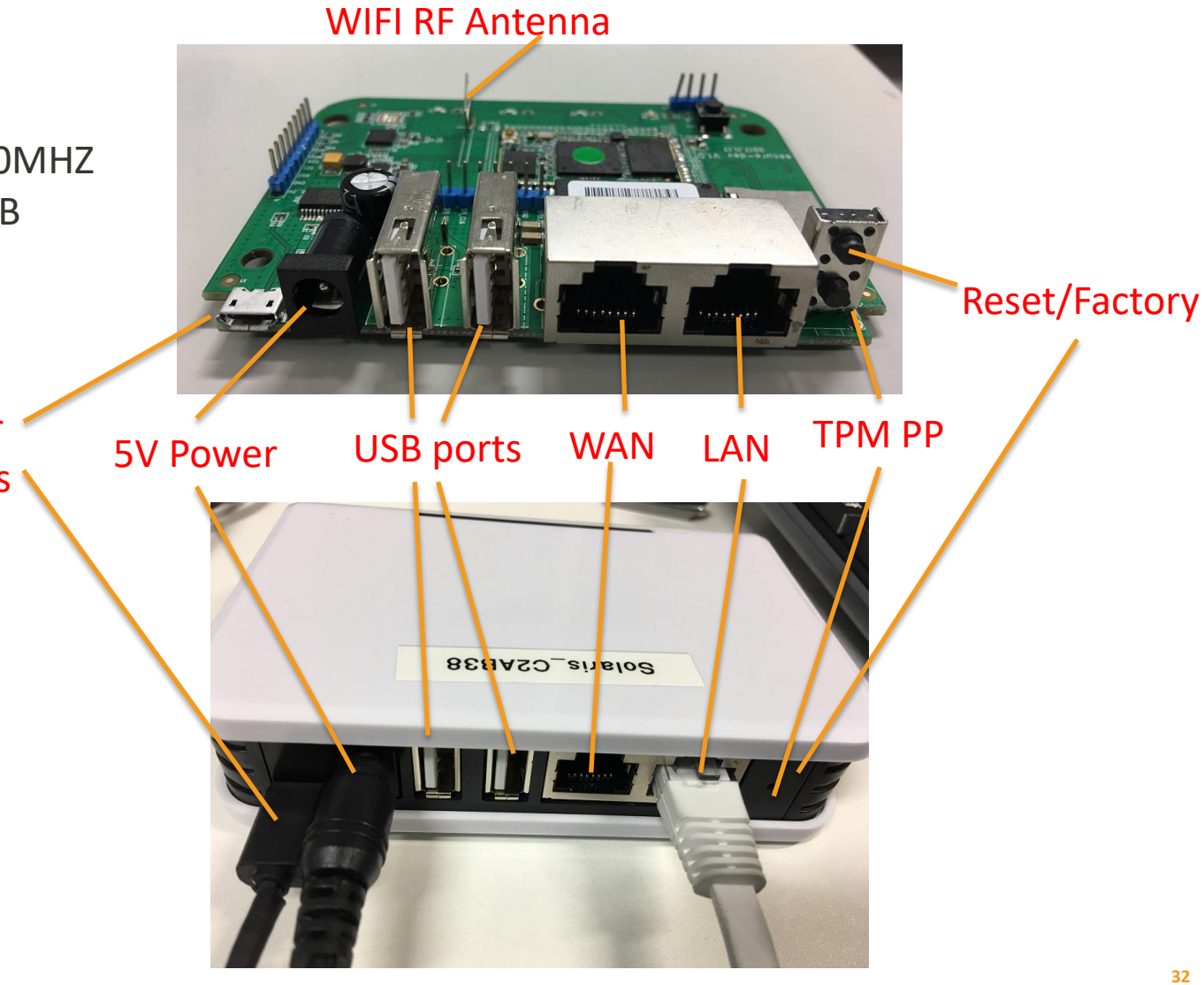




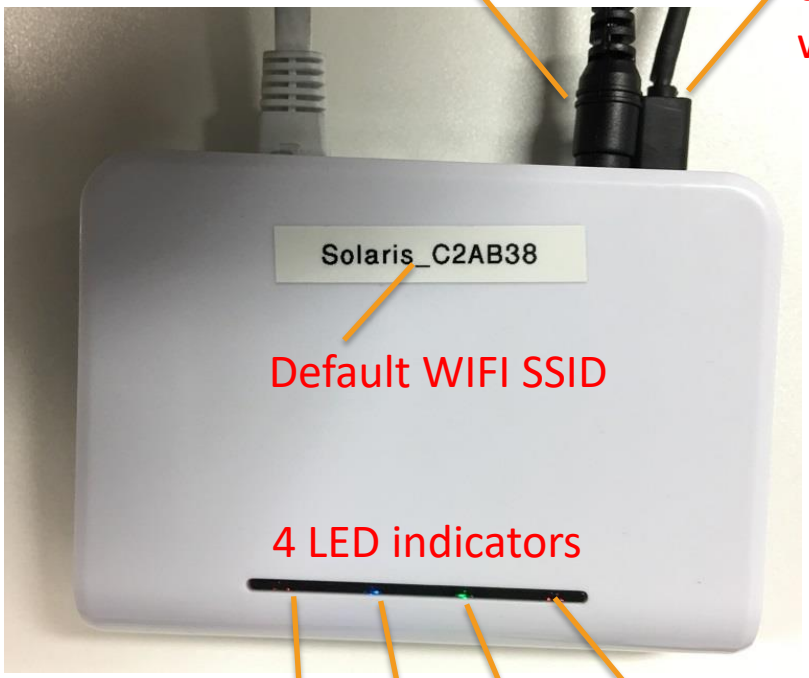
MT7688 IoT Gateway Set – Side View

Basic Info:

MT7688 MIPS 500MHZ
DDR2 RAM 128MB
Flash 64MB



MT7688 IoT Gateway Set – Top View



Sub-Systems Information

MT7688 Applications

MT7688 Chipset Information

- High Level Spec
  - MIPS24KEc 580 MHz with 64 KB I-Cache and 32 KB D-Cache
  - Supports up to 256MB RAM
  - 1T1R 2.4 GHz with 150 Mbps PHY data rate
  - Legacy 802.11b/g and HT 802.11n modes
  - 1-port 10/100 FE PHY
  - SD-XC, eMMC, I2C, PCM, I2S(192K/24bits), PWM, SPI master/slave, UART lite, JTAG and GPIO

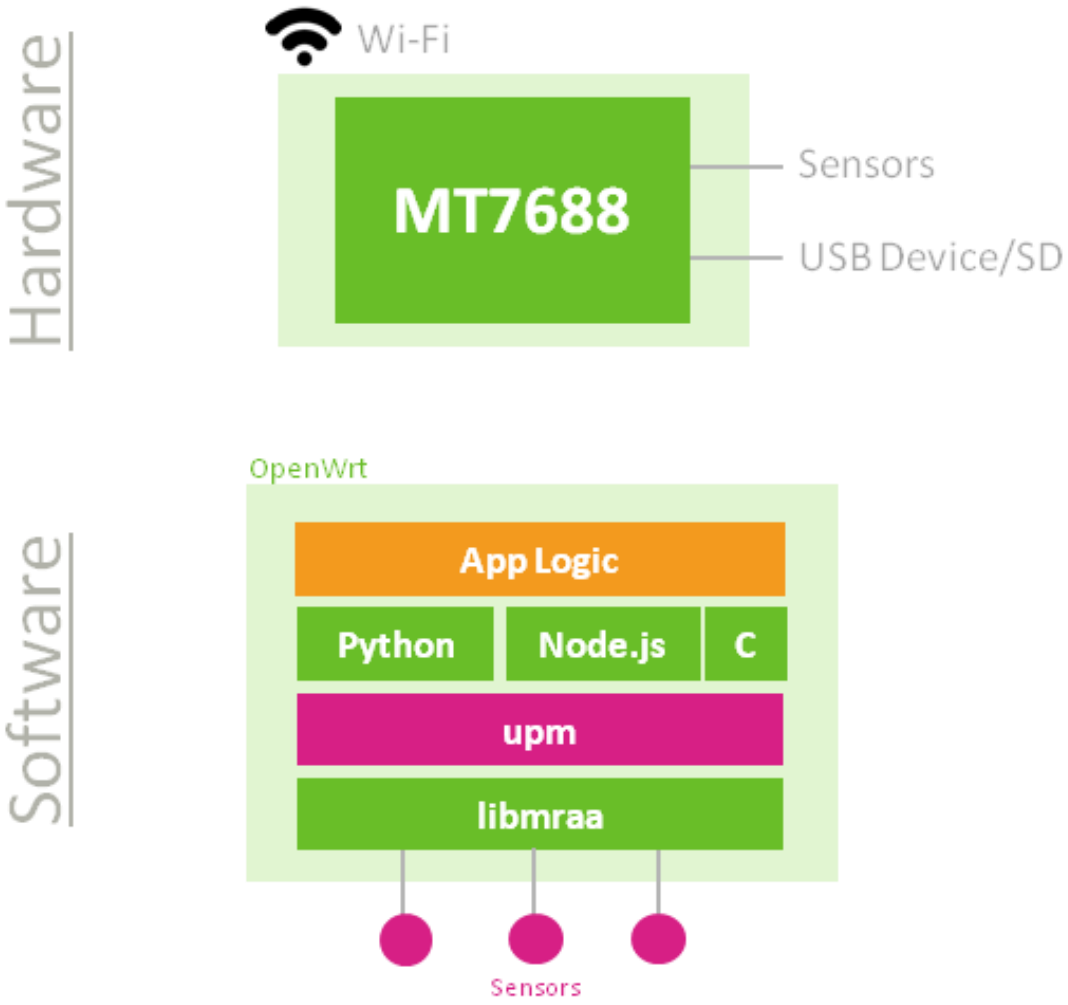
MT7688 Chipset Information

- Key features:

Processor Core	MIPS24KEc
Clock	580MHz
Package	DR-QFN156 (12mmx12mm)
Connectivity	1T1R 802.11n 2.4GHz Wi-Fi 10/ 100M Ethernet
RAM	Supports up to 256MB of external 16-bit DDR1/ DDR2 (193MHz) memory
External Flash Storage	SPI flash offering 3B addr mode (max 128MBit) and 4B addr mode (max 512MBit)
External Storage	SD-XC (Class 10)
Peripherals	USB 2.0 host, I2C, I2S, SPI, PWM, UART, GPIO, PCIe and eMMC

- Detail information can be found in
  - https://labs.mediatek.com/en/chipset/MT7688

MT7688 Software Stack



Infineon OPTIGA™ Trust B Turnkey Authentication

Strong Asymmetric Cryptographic Engine

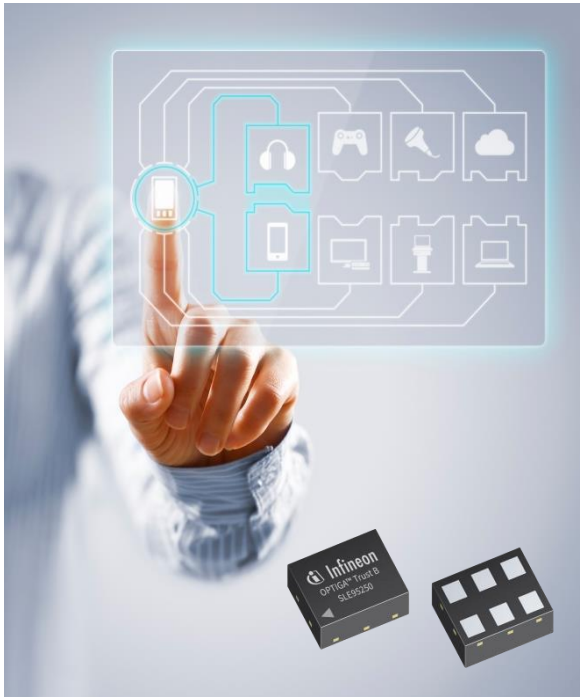
- Elliptic Curve Cryptography (131 bit key)
- Unique 96 bit identifier (UID)
- Public key certified by ODC-163 based digital certificate
- Optional kill feature

Protected Memory

- 512 bits lockable NVM
- Integrated Lifecycle Counter

Easy to Implement

- Full Turnkey Solution with Two Preloaded Key Pairs
- Host Code Provided
- Simple Single Wire Interface



Product Details

Programing	Turnkey	Interface	SWI
OS	N/A	Interface Speed	500kbps
Memory	512 b	Package	TSNP6
Cryptography	ECC131	Size	1.5 x 1.1 mm

More Info:

www.infineon.com/optiga-trust

Infineon OPTIGA™ TPM v1.2 and 2.0 for Highest Level of Certified Platform Protection

Trusted Platform Module: Secure your Software and Data

›Strong Authentication of Platform and Users
- Unique embedded Endorsement Certificate

›Secure Storage and Management of Keys and Data

›Platform protection for embedded systems
- Measured/Trusted Boot

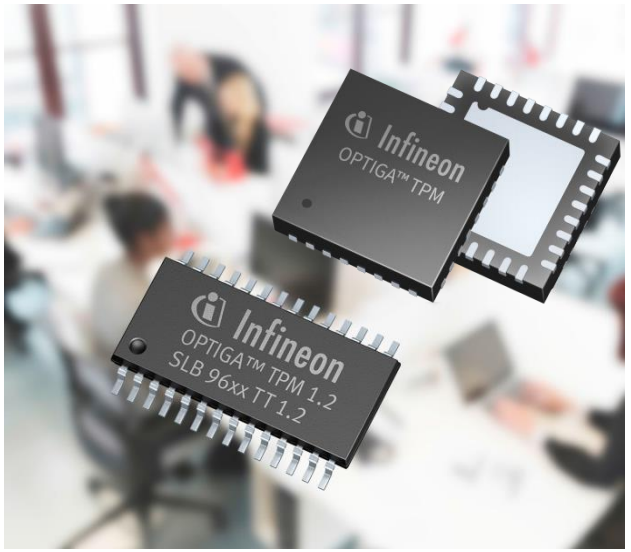
›RNG, Tick-Counter, Dictionary Attack Lock-out

›Built-in algorithms including RSA, ECC, SHA-256

Certified & Standardized Security

›Official TPM product listed at Trusted Computing Group (TCG)

›Independently security evaluated and certified: According to the international standard Common Criteria



Applications:

›Embedded Devices
- Industrial, Medical, Networking, Transport, Gaming etc.

›PC and Mobile Computing

›Intel x86, ARM platforms and others

More Info:

www.infineon.com/tpm

www.trustedcomputinggroup.org

Infineon OPTIGA TPM products

Product	TPM	Interface	Domain
SLB 9645	TPM 1.2	I2C	Embedded systems, non-x86 architectures
SLB 9660	TPM 1.2	LPC	PC-based systems, x86 architectures
SLB 9665	TPM 2.0		
SLB 9670	TPM 1.2	SPI	PC-based systems, x86 architectures embedded systems, non-x86 architectures
SLB 9670	TPM 2.0	SPI	