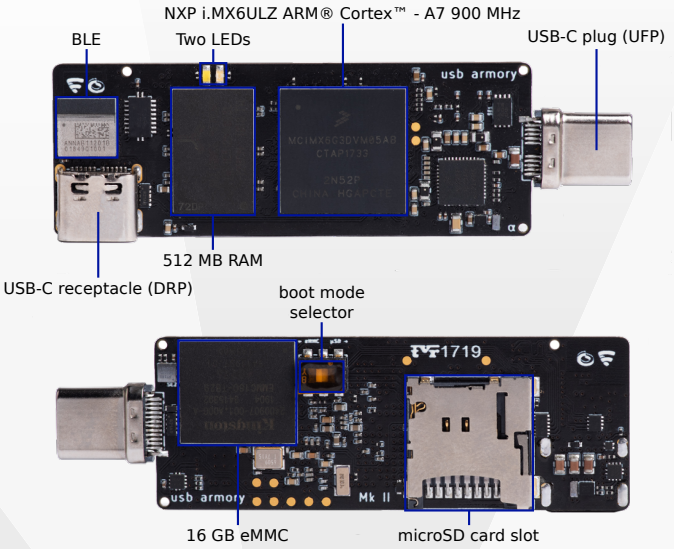
USB ARMORY MK II

The USB armory from F-Secure is an open source hardware design, implementing a flash drive sized computer.

Specifications

- **NXP ARM® Cortex™-A7 SoC: i.MX6ULZ 900 MHz or i.MX6UL 528 MHz**
- **RAM: 512 MB or 1 GB DDR3 • Flash memory: 16 GB eMMC**
- **USB powered (<500 mA) with compact form factor (65 x 19 x 6 mm)**
- **USB 2.0 over USB-C: DRP receptacle (host/device), UFP plug (device)**
- **Secure boot (HAB) and storage (SNVS), secure RAM (BEE on i.MX6UL only)**
- **Secure elements: Microchip ATECC608A and NXP A71CH**
- **microSD card slot**
- **Bluetooth module: u-blox ANNA-B112 BLE**
- **Debug accessory support for CAN (i.MX6UL only), UART, GPIO, SPI, I²C**
- **Supported by standard Linux kernels and distributions**
- **Supported by TamaGo for bare metal Go applications**
- **Open Hardware & Software**



Introduction

The compact USB powered device is a Single Board Computer which provides a platform for developing and running a variety of applications, thanks to its capabilities and unique form factor.

The features of the USB armory System-on-a-Chip (SoC) and security elements empower developers and users with a fully customizable USB trusted device for innovative applications.

Applications

The capability of implementing arbitrary USB devices in combination with the USB armory speed, the security features and the flexible and customizable operating environments, makes the USB armory the ideal platform for all kinds of personal security applications.

The transparency of the open and minimal design for the USB armory hardware facilitates auditability and greatly limits the opportunity and scope of supply chain attacks.

The secure boot feature allows users to fuse verification keys that ensure only trusted firmware can be ever executed and/or decrypted on a specific USB armory board.

The support for ARM® TrustZone®, the SoC built-in security features and external security elements, allows developers to engineer custom trusted platform modules of all kind.

The USB armory is a prime platform for the following applications:

- Encrypted storage solutions
- Hardware Security Module (HSM)
- Enhanced smart cards
- Electronic vaults (e.g. cryptocurrency wallets) and key escrow services
- Authentication, provisioning, licensing tokens
- USB firewall

Resources

- Documentation: **https://github.com/f-secure-foundry/usbarmory/wiki**
- Product page: **https://f-secure.com/en/consulting/foundry/usb-armory**
- TamaGo: **https://github.com/f-secure-foundry/tamago**

TamaGo

On top of standard support for rich operating environments, such as Linux distributions, the USB armory Mk II is directly supported by TamaGo, a framework that provides execution of unencumbered Go applications on bare metal ARM System-on-Chip (SoC) components.

TamaGo allows a dramatic reduction of the attack surface of embedded systems firmware by removing any runtime dependency on C code and/or Operating Systems.

F-Secure Foundry

The USB armory is created by F-Secure Foundry: **https://foundry.f-secure.com**

We live in a physical as well as digital world. Secure your hardware from conception to completion with world-class testing, engineering, and implementation.

Security features

Name	Use	Variants
HABv4	Secure Boot	all
RNGB	TRNG	only i.MX6ULZ
DCP	Cryptographic acceleration	only i.MX6ULZ
CAAM	Cryptographic acceleration, TRNG	only i.MX6UL
SNVS	Secure Non-Volatile Storage	all
BEE	On-the-fly external RAM encryption	only i.MX6UL
TZ	ARM® TrustZone®	all
ATECC	External cryptographic co-processor	all
A71CH	External cryptographic co-processor	all
RPMB	Protected flash memory region	all

Ordering information

Standard orders	
UA-MKII-ULZ-512M	USB armory Mk II • i.MX6ULZ 900 MHz • 1 GB RAM • enclosure
UA-MKII-DA	Debug accessory for the USB armory Mk II

Custom/bulk orders	
UA-MKII-UL-512M	USB armory Mk II • i.MX6UL 528 MHz • 512 MB RAM
UA-MKII-UL-1G	USB armory Mk II • i.MX6UL 528 MHz • 1 GB RAM
UA-MKII-ULZ-1G	USB armory Mk II • i.MX6ULZ 900 MHz • 1 GB RAM
UA-MKII-ENC	Enclosure for the USB armory Mk II

Resellers: **https://github.com/f-secure-foundry/usbarmory/wiki#purchasing**
Custom/bulk orders, support inquires: **usbarmory@f-secure.com**