F-SECURE FOUNDRY

We live in a physical as well as digital world.

F-Secure Foundry mission is to secure embedded products from conception to completion with world-class testing, engineering, and implementation.

We are breakers and makers, testing and building software and hardware products from the ground up since 2005.

This has given us a pragmatic engineering mindset that makes those products not only effective and secure, but practical to implement in your organization.

The USB armory is F-Secure Foundry own creation, built from the ground up, to showcase its capabilities and enable innovative security applications.

foundry.f-secure.com
USB ARMORY MK II

The USB armory is the world smallest secure computer.

It can safeguard data and run trusted applications, preventing unauthorized access or execution.

Minimal attack surface, vast performance and capabilities.


Fits right in your pocket, your laptop, your servers.
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 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)
- Key escrow services
- Authentication, provisioning, licensing tokens
- USB firewall

Specifications

- NXP ARM® Cortex™-A7 SoC: i.MX6ULZ 900 MHz or i.MX6UL 528 MHz
- RAM: 512 MB or 1 GB DD3
- Flash memory: 16 GB eMMC
- USB 2.0 over USB-C: DRP receptacle (host/device), UFP plug (device)
- 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

Bespoke Transparency

The USB armory has been developed entirely in-house by F-Secure Foundry and is manufactured in Italy.

The schematics and layout are open to the public as well as its core software, drivers and tools.

This gives unparalleled transparency to all customers.
The USB armory incorporates a vast number of features that can support a wide variety of security architectures. Its capabilities allow the safe storage of data as well as the trusted execution of operating environments and their applications, natively on the device itself.

Beyond simple smartcards or security tokens, the USB armory is a personal, self-contained, secure server.

With standard TCP/IP over USB or Bluetooth connectivity the USB armory can be easily interfaced with.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Use</th>
<th>Variants</th>
</tr>
</thead>
<tbody>
<tr>
<td>HABv4</td>
<td>Secure Boot</td>
<td>all</td>
</tr>
<tr>
<td>RNGB</td>
<td>TRNG</td>
<td>only i.MX6ULZ</td>
</tr>
<tr>
<td>DCP</td>
<td>Cryptographic acceleration</td>
<td>only i.MX6ULZ</td>
</tr>
<tr>
<td>CAAM</td>
<td>Cryptographic acceleration, TRNG</td>
<td>only i.MX6UL</td>
</tr>
<tr>
<td>SNVS</td>
<td>Secure Non-Volatile Storage</td>
<td>all</td>
</tr>
<tr>
<td>BEE</td>
<td>On-the-fly external RAM encryption</td>
<td>only i.MX6UL</td>
</tr>
<tr>
<td>TZ</td>
<td>ARM® TrustZone®</td>
<td>all</td>
</tr>
<tr>
<td>SE050</td>
<td>External cryptographic co-processor</td>
<td>all</td>
</tr>
<tr>
<td>RPMB</td>
<td>Protected flash memory region</td>
<td>all</td>
</tr>
</tbody>
</table>

The HAB feature enables on-chip internal Boot ROM authentication of initial bootloader (i.e. Secure Boot) with a digital signature, establishing the first trust anchor for code authentication.

The CAAM (i.MX6UL) and RNGB (i.MX6ULZ) provide true random number generation for cryptographic operations.

The CAAM (i.MX6UL) and DCP (i.MX6ULZ) provide cryptographic acceleration for encryption and hashing functions.

The built-in Bluetooth (BLE) module and the external microSD slot, in combination with the security features, allow secure wireless communication and storage expansion.

F-Secure Foundry provides drivers and tools for all USB armory security features and use cases.

Our consulting services enable porting existing customer applications on the USB armory secure environment as well as the bespoke design and implementation of innovative applications.

The SNVS (Secure Non-Volatile Storage) enables encrypted storage of arbitrary data using unique keys.

A device specific random 256-bit OTPMK key is fused in each SoC at manufacturing time, this key is unreadable and can only be used by the CAAM (i.MX6UL) or DCP (i.MX6ULZ) for AES encryption/decryption of user data.

Combined with Secure Boot (HAB) this allows complete lockdown of data through a trusted application.

The BEE is included only in boards mounting the i.MX6UL SoC, it supports on-the-fly (OTF) AES-128 (ECB or CTR) encryption/decryption on the AXI bus, allowing OTF DRAM encryption.

The NXP SE050 features hardware acceleration for elliptic-curve cryptography as well as hardware based key storage.

The eMMC RPMB features allows replay protected authenticated access to flash memory partition areas, using a shared secret between the host and the eMMC.
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 built-in Bluetooth (BLE) capability enables communication outside the USB ports, allowing authentication and interaction with mobile devices.

The USB armory breaks the conventional models of encrypted drives or security tokens, by providing a self-contained secure computer.

The execution of cryptographic and security operations, sensitive data and keys, remain on the device itself which can interact securely with its connected hosts or clients.

The USB armory does not merely take part in security operations, such as conventional smartcards or security elements, but rather executes and contain all of them within its core.

Opposed to traditional USB devices, the USB armory can authenticate peers on its own and refuse untrusted connections.

CONSUMER

- Encrypted storage solutions
- Cryptocurrency wallet
- Authentication token
- Secure password manager

ENTERPRISE

- Hardware Security Module
- Secure document store/sharing
- Enterprise authentication token
- Trusted Execution Environment

OEM

- Licensing server
- Secure device provisioning
- PKI / CA services

RESEARCH

- Low level USB testing
- Red Teaming implant
- Embedded development
**TamaGo**

In addition to native support for standard operating environments, such as Linux distributions, the USB armory is directly supported by TamaGo, an F-Secure Foundry developed framework that provides execution of unencumbered Go applications on bare metal ARM® System-on-Chip (SoC) processors.

TamaGo allows a dramatic reduction of the attack surface by removing any dependency on memory-unsafe languages (e.g. C), Operating Systems and third party libraries.

Project page:  
https://github.com/f-secure-foundry/tamago

**GoKey**

The GoKey application implements a **USB smartcard with innovative properties**. Featuring an SSH based management interface, the card provides a **dramatically improved security model** over traditional smartcards. By leveraging on the TamaGo framework, GoKey is written and executed with only high-level code, minimal dependencies and a memory-safe environment.

<table>
<thead>
<tr>
<th></th>
<th>Trust anchor</th>
<th>Data protection</th>
<th>Runtime</th>
<th>Application</th>
<th>Requires tamper proofing</th>
<th>Encryption at rest</th>
</tr>
</thead>
<tbody>
<tr>
<td>traditional smartcard</td>
<td>flash protection</td>
<td>flash protection</td>
<td>JCOP</td>
<td>JCOP applets</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>USB armory with GoKey</td>
<td>secure boot</td>
<td>SoC security element</td>
<td>TamaGo</td>
<td>Go application</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Project page:  
https://github.com/f-secure-foundry/gokey
The GoTEE framework implements a Trusted Execution Environment (TEE) bringing Go memory safety, convenience and capabilities to bare metal execution within ARM® TrustZone® Secure World.

GoTEE allows concurrent instantiation of bare metal trusted applets (whether written as TamaGo unikernels or freestanding programs such as Rust or C ones) along side an isolated OS such as Linux.

An OP-TEE compatibility layer for Trusted Applets API and Normal World kernel driver is available.

Project page: https://github.com/f-secure-foundry/GoTEE
Example use cases

Armory Drive

The USB armory performs transparent encryption/decryption of the user microSD card.

Authorization happens over Bluetooth to ensure safe operation even on untrusted laptops.

Project page: https://github.com/f-secure-foundry/armory-drive

Remote Hardware Security Module

When hosting facilities cannot be trusted, the USB armory, plugged on a server, complements its potentially unsafe environment with self-contained, tamper proof, HSM services.

Remote peers can authenticate the USB armory and use it, while the server remains an unprivileged party.

The server itself can also use the USB armory HSM services for CA/PKI or any other cryptographic purpose, without having access to protected keys.

The USB armory advantage

No other platform combines so many security features, performance, expandability, customization, and transparency in the tiniest of form factors. The USB armory is uniquely placed in the market.

Its security architecture outperforms traditional smartcards, HSMs, tokens and other secure devices.

<table>
<thead>
<tr>
<th></th>
<th>Trust anchor</th>
<th>Versioning anchor</th>
<th>Data protection</th>
<th>Runtime</th>
<th>Applications</th>
<th>Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>smartcard</td>
<td>flash protection</td>
<td>none</td>
<td>flash protection</td>
<td>JCOP</td>
<td>JCOP applets</td>
<td>poor</td>
</tr>
<tr>
<td>traditional HSM</td>
<td>vendor dependent</td>
<td>vendor dependent</td>
<td>flash protection</td>
<td>unknown</td>
<td>Java/C (typ.)</td>
<td>good</td>
</tr>
<tr>
<td>FPGA based devices</td>
<td>bitstream encryption</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>RTL</td>
<td>good</td>
</tr>
<tr>
<td>traditional security token</td>
<td>flash protection</td>
<td>eMMC/NAND/crypto acc.</td>
<td>flash protection</td>
<td>RTOS</td>
<td>low level C/C++ code</td>
<td>medium</td>
</tr>
<tr>
<td>traditional encrypted drive</td>
<td>none</td>
<td>none</td>
<td>MCU crypto acc.</td>
<td>N/A</td>
<td>N/A</td>
<td>medium</td>
</tr>
<tr>
<td>USB armory</td>
<td>secure boot</td>
<td>eMMC/NAND/crypto acc.</td>
<td>SoC crypto acc.</td>
<td>any</td>
<td>any language</td>
<td>good</td>
</tr>
</tbody>
</table>
Resources

Ordering information

<table>
<thead>
<tr>
<th>Standard orders</th>
<th>Order Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UA-MKII-ULZ-512M</td>
<td>USB armory Mk II • i.MX6ULZ 900 MHz • 512 MB RAM • enclosure</td>
<td></td>
</tr>
<tr>
<td>UA-MKII-DA</td>
<td>Debug accessory for the USB armory Mk II</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Custom/bulk orders</th>
<th>Order Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UA-MKII-UL-512M</td>
<td>USB armory Mk II • i.MX6UL 528 MHz • 512 MB RAM</td>
<td></td>
</tr>
<tr>
<td>UA-MKII-UL-1G</td>
<td>USB armory Mk II • i.MX6UL 528 MHz • 1 GB RAM</td>
<td></td>
</tr>
<tr>
<td>UA-MKII-ULZ-1G</td>
<td>USB armory Mk II • i.MX6ULZ 900 MHz • 1 GB RAM</td>
<td></td>
</tr>
<tr>
<td>UA-MKII-ENC</td>
<td>Enclosure for the USB armory Mk II</td>
<td></td>
</tr>
</tbody>
</table>

Custom/bulk orders, support inquiries: usbarmory@f-secure.com

---

F-Secure Foundry

The USB armory is created by F-Secure Foundry.

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

foundry.f-secure.com
ABOUT F-SECURE

Nobody has better visibility into real-life cyber attacks than F-Secure. We’re closing the gap between detection and response, utilizing the unmatched threat intelligence of hundreds of our industry’s best technical consultants, millions of devices running our award-winning software, and ceaseless innovations in artificial intelligence. Top banks, airlines and enterprises trust our commitment to beating the world’s most potent threats.

Together with our network of the top channel partners and over 200 service providers, we’re on a mission to make sure everyone has the enterprise-grade cyber security we all need. Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd.

f-secure.com/business | twitter.com/f-secure | linkedin.com/f-secure