FILAMENT

Blocklet USB Enclave

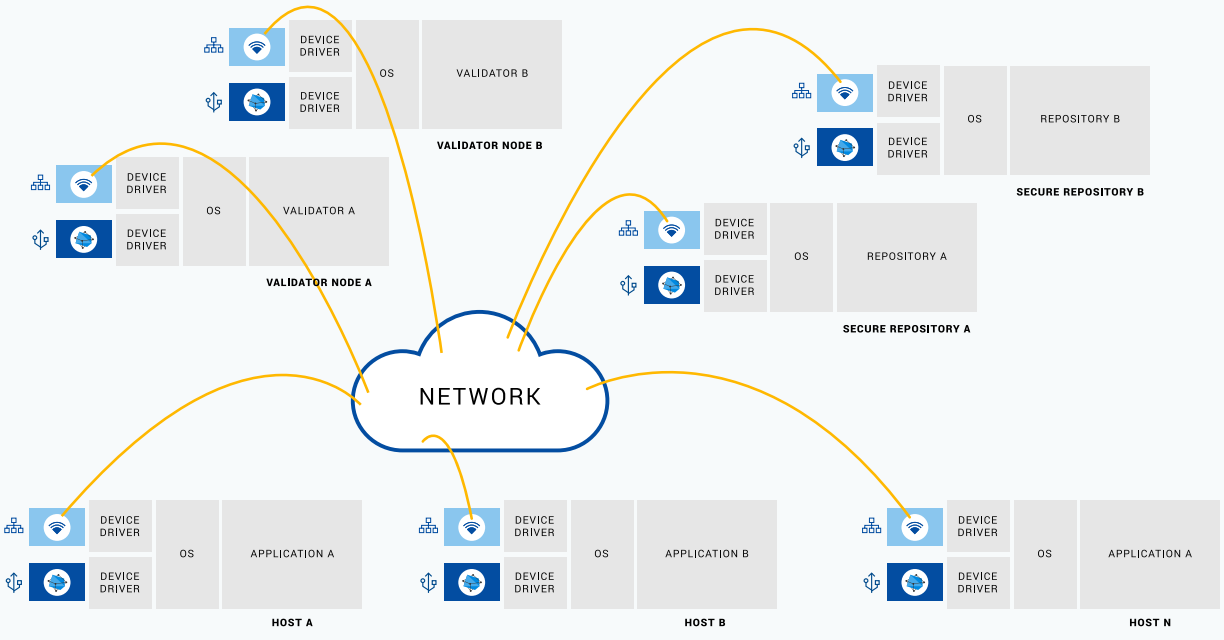
DATA SHEET

Overview

The Blocklet™ Universal Serial Bus (USB) Enclave provides host systems with secure identity and authentication services. The device installs in a standard Type A USB 2.0 host port and interfaces to a host device driver for configuration and subsequent operational services.

During an installation pairing-process, the Blocklet USB Enclave and supported host permanently bond, thereby establishing an immutable unique identity for the combined devices. The bonding enables supported configurations to engage in sensitive transactions requiring uncompromised device identification and digital signatures. Attempts to use a Blocklet USB Enclave with any host other than the host the USB device was originally bonded with will be unsuccessful. Finally, USB device applications include, but are not limited to, digital asset verification and transfer operations such as traditional Blockchain, Ethereum, etc. – i.e. secure digital repository applications generally referred to as Digital Ledger applications.

BLOCKLET USB ENCLAVE



CONCEPTUAL BLOCKLET USB ENCLAVE DEPLOYMENT

Blocklet USB Enclave supported hosts participate in digital asset applications using digitally signed transactions that USB devices facilitate. Note that Secure Repositories only commit repository updates when all associated transactions have been successfully authorized according to the Secure Repository's rules. Occasionally, this requires a Validator system to resolve consensus contention. A Secure Repository may have multiple associated Validator systems.

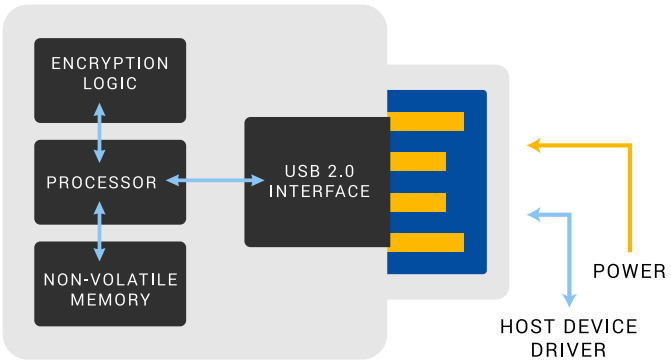
Architecture Overview

The Blocklet USB Enclave incorporates a low power M0+ class ARM processor operating at 48MHz, 2 MBytes of NOR-Flash memory, and a cryptographic accelerator. Among other things, the Flash memory contains operational firmware installed during hardware manufacturing processes, transient host data, and cryptographic data values involved in providing on-demand host services. Some user Flash address ranges are protected from change. Filament can provide operational firmware updates for inadvertent firmware error resolution. To prevent physical intrusion, Filament manufactures industrial-strength, sealed USB enclosures and encases internal components in tamper-evident substances to impede disassembly and data examination. Should such a disassembly occur, any data examination effort will only result in encrypted data extraction. A Blocklet USB Enclave receives all power from standards-compliant USB 2.0 interfaces.

FEATURE	SPECIFICATION
Host Connection	USB 2.0
Host Connector	Type A
Dimensions	18.4mm W x 39.7mm L (.72" W x 1.56" L)
Amperage	<100 mA
Maximum Watts Consumed	0.5 W
Operating Conditions	-55° C to 85° C. (-67° F to 185° F) Non-condensing moisture
Encrypted and Hashing Acceleration Support	• AES256 • Elliptic Curve secp256k1 • FIPS186-3 Elliptic Curve Digital Signature (ECDSA) • FIPS SP800-56A Elliptic Curve Diffie-Hellman (ECDH) Algorithm • NIST Standard P-256 Elliptic Curve • SHA-256 Hash Algorithm with the HMAC Option

Device Driver Support

Filament provides sample C source code device drivers for device driver creation. (Note: It may be possible to access Blocklet USB Enclave services using standard USB Communication Device Class services.)



BLOCKLET USB ENCLAVE ARCHITECTURE

Programming

Blocklet USB Enclaves contain embedded firmware and unique values that the manufacturing process loads into Flash memory. Using unique additional information values Filament provides its customers, this firmware enables the USB device to bond with a host. The bonding process produces a unique 72-bit bonding identifier (one of 2^{72}) which the collective hosts initially use to grant a new USB device supported machine admission into the larger processing complex. Thereafter this unique value helps ensure uncompromised, subsequent transaction messaging authenticity involving any similarly USB device-bonded host within the system. Since there are an estimated 2^{60} grains of sand in the world, Blocklet USB Enclaves have over 4,096 (2^{12}) times as many possible values as there are grains of sand in the world, thereby providing uncompromising digital asset system participant authentication.

Host Application Blocklet USB Enclave Interfacing

Host-bonded applications access the Blocklet USB Enclave services through standard programming system calls invoking a Filament-defined Application Programming Interface (API). To obtain USB device services, a host program API call invokes Filament-licensed support modules that Filament supplies in a Software Development Kit (SDK) as C Language source code files. Programs written in languages other than C, such as Python, can access the SDK modules using standard, well known language-specific interfacing techniques.

FILAMENT

www.filament.com | hello@filament.com | +1.775.434.0095