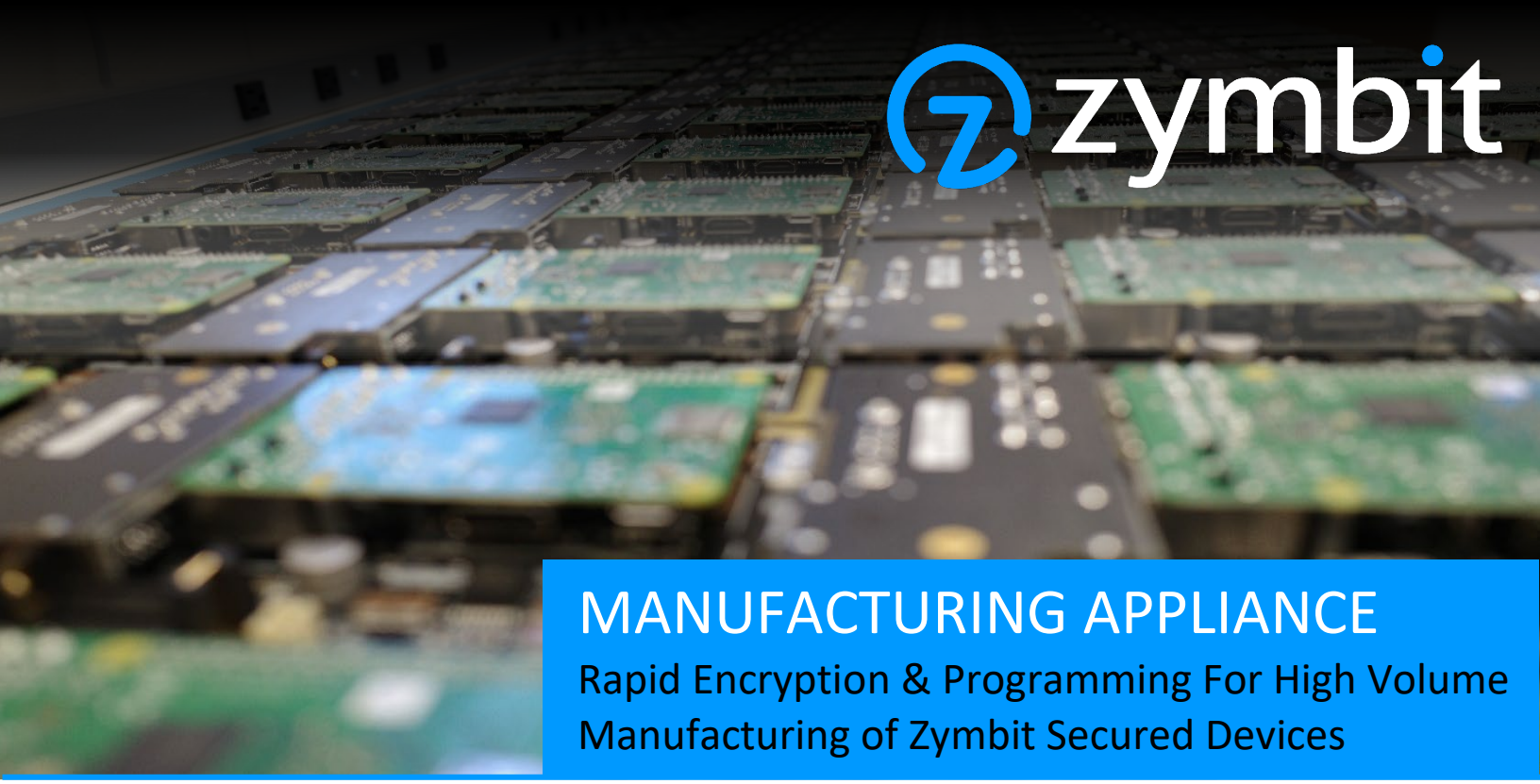


MANUFACTURING APPLIANCE

Rapid Encryption & Programming For High Volume Manufacturing of Zymbit Secured Devices

Key Features

- Encrypt and program hundreds of Zymbit HSM secured devices per day.
- Unique encryption key for each device, generated on device, on the fly.
- Parallel programming of 4, 8, 12 devices.
- Integrates with customer provisioning and secure image download frameworks.
- Easily operated by manufacturing technicians.

Efficient AND Secure

Producing thousands of encrypted devices can be time consuming and error-prone especially if each device requires a uniquely encrypted file system. Yet using a single manufacturing key across a batch of devices can introduce obvious vulnerabilities.

The Zymbit manufacturing appliance solves these problems and delivers an efficient **and** secure workflow to encrypt and provision each device uniquely.

Multiple Levels of Trust

A typical manufacturing supply chain involves multiple players, who are often remote or not under the direct supervision of the product owner. To support the secure manufacture of OEM products by third party manufacturers, it is essential that the operating software is injected through an authenticated and encrypted communication channel into a uniquely authenticated device with uniquely encrypted file system.

The Zymbit manufacturing appliance can support multiple levels of operator authentication, device authentication, communication authentication, batch authorization and software image verification.

SECURED BY ZYMBIT

The manufacturing appliance will support all Zymbit security modules when used together with those single board computers and Linux OS versions supported by Zymbit. Check community.zymbit.com for currently supported SBC's and operating systems.

Device Measurement and Identity

Zymbit security modules enable remote attestation of host device hardware configuration:

- Unique ID token based upon multiple device-specific measurements
- Cryptographically derived ID token never exposed
- Custom input factors available to OEMs
- ID tokens bound to host permanently for production, or temporarily for development
- Changes in host configuration trigger local hardware & API responses, policy dependent

File System Encryption With Device Unique Key

Zymbit security modules provide a cryptographic engine featuring some of the strongest commercially available cipher functions to encrypt, sign and authenticate data:

- Strong cipher suite includes ECDSA, ECDH, AES-256, SHA256
- AES-256 encrypt/decrypt data service
- Integration with TLS client certificate, PKCS11
- TRNG - true random number generator, suitable seed for FIPS PUB 140-2, 140-3 DRNG.

Key Generation and Services

Zymbit security modules generate and store key pairs in tamper resistant silicon to support a variety of secure services:

- 32 key slots, pre-defined and user available
- Cryptographic primatives
  - ECC KOBLITZ P-256 (secp256k1), ECC NIST P-256 (secp256r1)
  - ECDSA (FIPS186-3), ECDH (FIPS SP800-56A)
  - AES-256 (FIPS 197), TRNG (NIST SP800-22)
- Private keys never exposed outside of silicon

Physical Tamper Detection Arm

Zymbit security modules monitor the physical environment for symptoms of physical tampering:

- Power quality monitor detects anomolies like brown-out events
- Optional perimeter integrity circuits detect breaks in user defined wire loops/mesh
- Accelerometer detects shock and orientation change events
- Event reporting and response according to pre-defined policies

Real Time Clock Verification

Zymbit security modules include a battery-backed real time clock to support off grid applications:

- 2-10 years operation, dependent upon external battery size.
- RTC clock service, available to client applications
- RTC/UTC anamoly alerts available with zymbit security services
- 20ppm accuracy (standard). Optional 5ppm accuracy (OEM feature, MOQ apply)

Secured by Zymbit Hadware Security Module

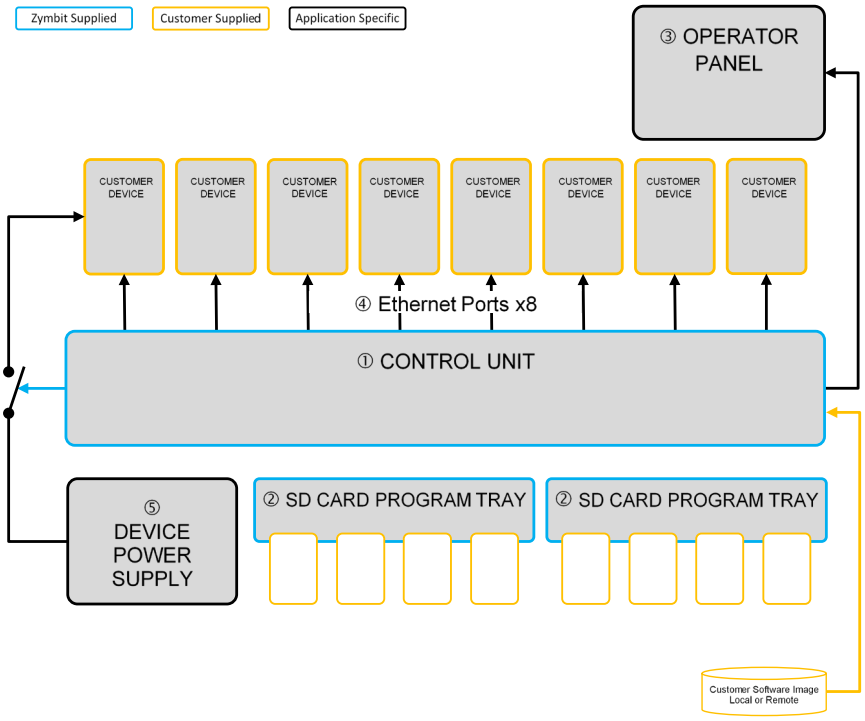
Zymbit security modules provide multiple layers of hardware security:

- Hard to penetrate dual secure-processor architecture
- Secure microcontroller supervises device multifactor identity / authentication and physical security.
- Secure microcontroller isolates secure element from host
- Secure elements from Microchip - ATECC608
- Hardware based cryptoengine and keystore

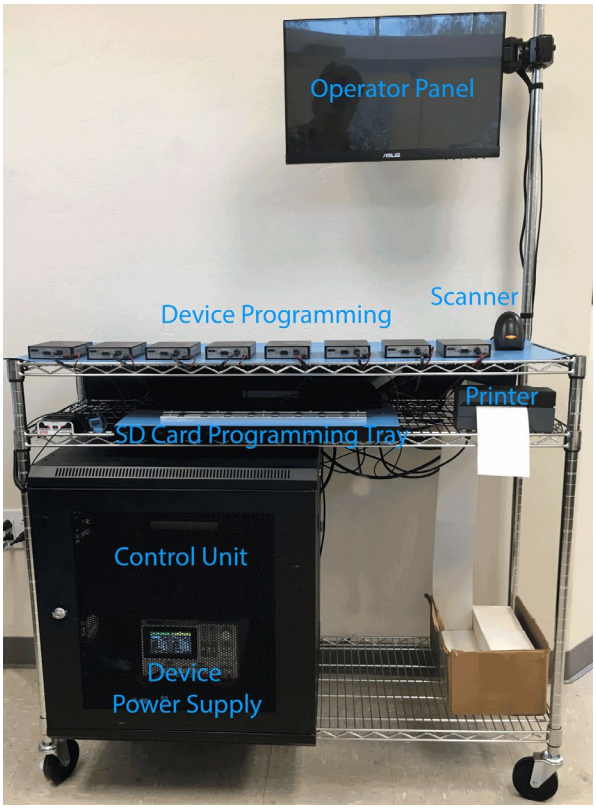
CONFIGURATION

Typical System Configuration

Each manufacturing appliance contains a control unit and SD Card programming trays. Additional components are added by the customer, or Zymbit, to meet specific device power and operator-interface requirements.



Rack Mounted Zymbit Manufacturing Appliance Example



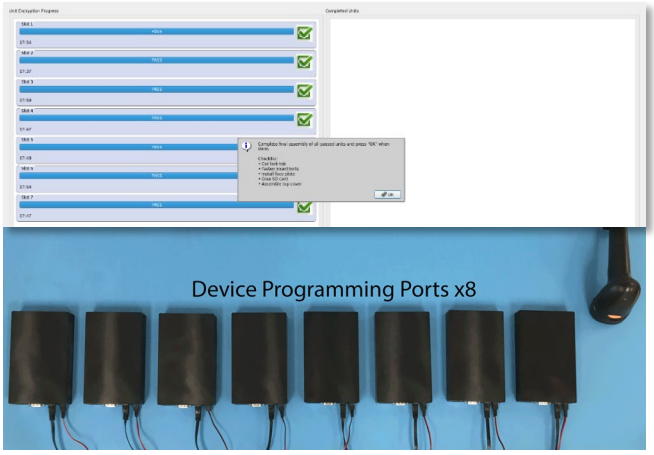
WORKFLOW

Typical Work Flow

	Process Step	*Notes*
1.0	Place SD card into programing tray	*manual, four and eight station trays available*
	⇩	
2.0	Sanitize SD card	*auto over-writes with random data, unique per instance*
	⇩	
3.0	Program Zymbit starter software image	*auto*
	⇩	
4.0	Move SD card to target system	*manual*
	⇩	
5.0	Bind SD card to target system	*auto, creates unique multi-factor ID (Pi + SD card + othe*
	⇩	
6.0	Create encrypted file system volume(s)	*auto*
	⇩	
7.0	Upload customer software image	*auto, from master image, or from cloud download*
	⇩	
8.0	Program customer software image	*auto, programs into encrypted file system*
	⇩	
9.0	Verify customer software image	*auto*
	⇩	
10.0	Cut lock-tab on Zymkey	*manual*
	⇩	
11.0	Close tamper circuit(s) – if applicable	*manual*
	⇩	
12.0	Arm tamper detect policy – one time	*Auto*
	⇩	
12.0	Remove device	*manual*
	⇩	
13.0	END	

Simple to Use Operator Interface

Sanitizing SD Cards with unique fuzzed data



Encrypt and program multiple devices in parallel

ORDERING OPTIONS

4, 8 or 12 Devices

The manufacturing appliance is available in three standard configurations: 4, 8 and 12 devices. For larger numbers of devices, contact Zymbit to discuss your specific application needs.

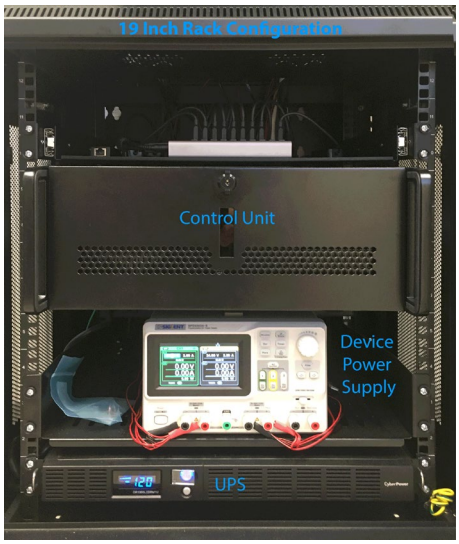
Buy or Lease

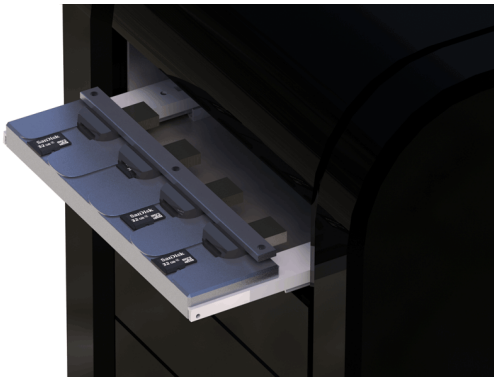
The manufacturing appliance can be purchased outright or leased from Zymbit. Leasing models provide a lower cost of entry and are based upon a time-of-use or per device pricing.

Rack or Desktop Format

The rack mounted manufacturing appliance is designed to be incorporated into a standard 19-inch-wide rack. It is usually combined with other equipment - such as power supplies, printers and UPS - that are related to the programming, assembly and final packaging and labeling of the target devices. Contact Zymbit engineering services to discuss your custom needs.

The desktop manufacturing appliance is a free-standing ATX format tower with internal 4 or 8 SD card programming tray.





DOCUMENTATION

Full documentation for the Manufacturing Appliance is available under NDA to qualified customers. Available documentation includes:

- Operator Manual
- Software Integration Guidelines
- CAD Footprint and mechanical Files

For more information, visit **www.zymbit.com/manufacturing-support**

zymbit