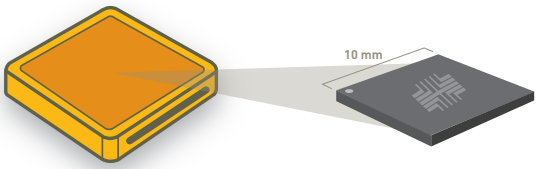
Pitney Bowes

Trusted Mobile Development Platform

Cryptographic Accounting Module (CAM) Hardware Security Module



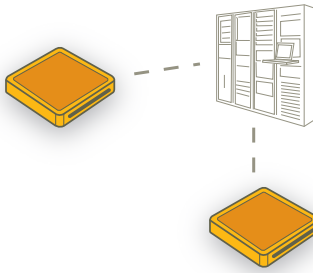
Embedded microcontroller and cryptographic co-processor

- Single chip solution – 10x10 mm 144 pin TFBGA
- Tamper detection and tamper responsive
- Meets FIPS 140-2 Level 3 + EFP Requirements
- Secure Real-Time Clock
- Secure Persistent Storage
- Programmable (ARM7 CPU)
- USB and Serial Interfaces
- Remote enable/disable
- Secure Software Download
- Remote audit and inspection
- Secure accounting registers
- High integrity financial transactions

Cryptographic Functions:

- RSA/DSA and Elliptic Curve Algorithms
- AES and DES
- Secure Random Number Generator

CAM SERVER Secure Infrastructure



Server can remotely manage millions of CAMs and works with multiple applications

Fully integrated Public Key Certificate Authority

- Issue device and server certificates
- Create unlimited security domains
- Secure field updates of certificates and keys
- CRL management

Secure Transaction Management

- Add/remove funds from devices
- Audit transaction history per-device
- Fraud analysis

Remote device management

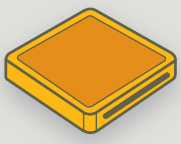
- Remote inspection
- Remote certificate and key updates
- Remote provisioning
- Remote software updates
- Device activation/deactivation

Scalable to support millions of remote devices

Secure Online and Off

The combination of the CAM and the CAM Server enables rapid deployment of secure applications.

When connected online, get industry standard algorithms with hardware acceleration and the assurance that keys and root certificates are never exposed in software.



When offline, get the assurance of tamper-responsive technology to ensure that keys and business logic remain protected.

ONLINE OFFLINE

First Modular Mobile Device Development Platform

That provides cryptographic processing, a secure time source, transaction management, remote security lifecycle management, and third party server validation.

Applications

Communications Security

- Secure channel with client-side certificates
- Standards compliant certificate infrastructure managed by the CAM server
- Key agreement performed within the tamper-responding crypto boundary

Secure Accounting

- Transfer funds or other units of value into/out of devices
- Perform remote audit of device transaction history
- Multi-phase commit ensures transaction integrity

Data Protection

- Industry standard public and symmetric key cryptography and digital signatures
- Secure key management
- Private keys never leave the tamper-responding boundary

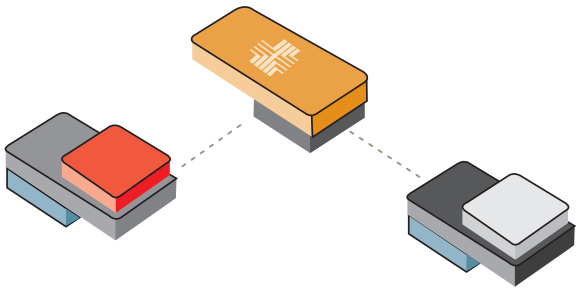
Secure Device Management

- Hardware security + a secure infrastructure enables trusted remote device management
- Secure software updates with digital signatures and time stamps
- Remote enable/disable of devices
- Remote provisioning

Technical Details

Algorithms Supported

- FIPS 186-2 compliant Public Key Crypto Engine (DSA, RSA, ECDSA)
- FIPS 180-2 compliant Hash Engine (160, 224, or 256 bit)
- FIPS 197 compliant AES Engine (256 bit)
- FIPS 46-3 compliant 3DES engine
- Hardware Random Number Generator
- Side channel attack resistance (SPA/DPA/TA)
- Active tamper detection and response circuit
- 3.3V design, 20mA when active



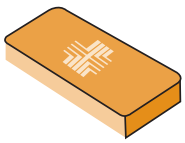
Pitney Bowes + bug labs = BUGsecure

NEW YORK, March 14, 2011 - Bug Labs, an open source hardware and software provider, and Pitney Bowes Inc. (NYSE: PBI) today announced the industry's first modular, mobile device development platform incorporating hardware-level security and security life-cycle management services. As a new addition to Bug Lab's flagship open source device prototyping platform, BUGsecure offers enterprises a flexible, trusted platform with the highest level of data protection and encryption available. Current devices on the market rely on software security, making them more vulnerable to breaches. BUGsecure provides a deeper level of security by fully protecting the device's hardware and operating system, not just its application software.

Read more on pb.com

Introducing BUGsecure, the combined power and functionality of the Bug Labs BUGbase 2.0 with an embedded tamper-responding security chip from Pitney Bowes.

- Integrated hardware security allows you to launch prototypes with live data
- Design with security from the start instead of as an afterthought



For more information contact us at: SecurePlatform@pb.com