The Cryptographic Accounting Module

The Cryptographic and Accounting Module (CAM) is an integrated circuit designed to provide assurance of the integrity and privacy of transactions. Within its tamper responding secure boundary, the CAM contains a real-time clock, transaction registers, a user management system, a cryptographic coprocessor and cryptographic key store. The integrity and privacy of data related to transactions/events is accomplished by employing the cryptographic functions supported by the CAM. In addition the CAM provides several mechanisms to restrict the use of the cryptographic functions based upon the passage of time or use of a resource.
The CAM is accessed through a USB interface. It is available packaged in three form factors: a single integrated circuit, a plug-in module with integrated support circuitry, and integrated within a BugLabs trusted mobile modular development system. Three interfaces have been developed for the plug-in module:

- A small box providing a standard USB interface
- A BugLabs module
- A rack mounted board that provides a USB interface to multiple CAM's (in development).

Cryptography

The CAM offers a number of cryptographic services to protect the source, integrity and privacy of data. The CAM contains an internal key store for each user.

Digital Signatures

Digital signatures provide source authentication (where did the data come from?) and data integrity (has the data been changed?). Digital signatures are created using a private key and verified using a public key. Internal CAM data can be included in the digital signature including: Date/Time, serial number, ascending and descending registers, transaction count, and username. External data sent into the CAM can be used as input to the digital signature. Digital signatures can be verified using the CAM's public key which is contained in an X.509 certificate stored within the CAM. The X.509 certificate can be stored in a database or transmitted along with the signature. The CAM is not necessary for verification.

A CAM can be used to verify a digital signature created by another device. The public key of the other device must be prepared for loading into the CAM (e.g., a server may provide an encrypted version of one CAM's public key to another CAM).

The CAM can load an external key pair that has been prepared for it (e.g., a server may provide an encrypted key pair to a CAM). This is useful for sharing a key pair between multiple CAM's.

Encryption

Encryption provides a mechanism to protect the privacy/disclosure of data.
The CAM can encrypt data for itself. This is useful for short or long term storage of data external to the CAM (e.g., locally on a PC, on a remote server).

The CAM can agree on an encryption key with another CAM to encrypt data for shared between the CAM's. This is useful for ensuring privacy of data transmitted from one CAM to another. It can also ensure that data encrypted by a CAM can be accessed if the CAM fails.
The CAM can agree on an encryption key with another device (e.g. a server).
The CAM can load an external encryption key that has been prepared for it (e.g. a server may provide an encrypted key to a CAM). This is useful for sharing a key between multiple CAM's.

Message Authentication Codes

Message authentication codes (MAC's) provide data integrity (has the data been changed?). MAC's are created and verified using a secret (symmetric) key. Since the MAC creator and verifier use the same key. MAC's do not provide source authentication.
The CAM can create MAC's for itself. This is useful to detect if data stored locally has changed (e.g., data stored external to the CAM on a local PC).
The CAM can agree on a MAC key with another CAM. This is useful for ensuring the integrity of data is maintained during transmission or storage.
The CAM can agree on a MAC key with another device.

Restricting Use

The CAM's functionality can be restricted in whole or in part based upon expiration periods, specific dates, use of a resource or a combination of the three. These restrictions are managed via a server infrastructure which performs manufacturing, cryptographic key management and CAM configuration management.

Time based

The CAM has an internal real-time clock. The value of the clock is set to GMT during CAM manufacturing. There are two mechanisms within the CAM that restrict use based upon the time stored within the CAM. The two mechanisms are independent and can be used simultaneously.
An expiration period can be set within the CAM. If the expiration period has passed, the CAM will not perform any cryptographic operations using user keys (communications with the infrastructure are not affected). The expiration period is renewed by a series of signed messages between the CAM and the infrastructure. The infrastructure checks the CAM status (register values) for consistency before renewing the expiration period.
Each key within the CAM is assigned an expiration date. Once a key has expired the CAM will not perform any operations using that key. The expiration of a key does not affect the use of other keys.

Accounting/Resource Based

The CAM contains three registers: an Ascending Register (increases as resource is expended, total of all resource expended for the life of the CAM), Descending Register (decreases as the resources is expended) and transaction counter (increments for each transaction). If the descending register is lower than the requested amount no digital signature operation will be performed. The descending register may be decreased by a variable amount during signature generation and a fixed amount during signature verification. A minimum debit amount may be

specified for signature generation. Both the minimum debit amount for signature generation and the fixed amount for verification may be zero. Typical uses for the descending register include funds (postage, tax payment…) or to limit use (decrement by 1 each time a document is signed). The CAM may be configured to increment the transaction count for each signature generation and/or each signature verification.

The infrastructure adds resources to a CAM's descending register by exchanging a set of digitally signed messages with the CAM.