CAPSTONE &

TESSERA

an Overview

Leon S. Scaldeferri

Office of Information Security Research[1]

NSA, R22

9800 Savage Rd.

Ft. Meade MD 20755-6000

(301) - 688 - 0293 /0289[fax]

em: lsscald@alpha.ncsc.mil

1. Opinions expressed in this paper are those of the author and do not represent the opinions or position of the FWUF or NSA.

Capstone Description:

The Capstone chip is a versatile single chip cryptographic engine providing both the new encryption/decryption standard, and public key exchange management plus many other cryptographic support functions. The Capstone chip can be used in many applications, from the public key systems to dedicated systems using the specific features of the chip. The chip can also be used for the Digital Signature and Verification with interactive key exchange and message authentication. The Capstone chip provides an all-around cryptographic solution for key exchange, authentication, and high-grade and high-speed communication link encryption.

The Capstone chip is designed using an Advanced RISC Machine's (ARM) processor, similar to the one used in the Apple Newton. The architecture is based on Reduced Instruction Set Computer (RISC) principles, and the instruction set and related decode mechanism are greatly simplified compared to microprogrammed Complex Instruction Set Computers. This simplification results in high instruction through put and cost-effective chip design. The Capstone chip can perform two main functions. First, the chip is a cryptographic engine that can perform digital signature, key exchange, hash, and encryption/decryption including various associated cryptographic functions. The cryptographic functions are controlled by an internal operating system, (O/S), on the chip. This cryptographic O/S is transparent to the user except for user-defined memory mapping for data handling. The second function of the Capstone chip is the use of the RICS processor as a general purpose microprocessor. It is designed to operate with any user-defined operating system. The user-defined operating system can be designed in accordance with the user's system requirements. The command set for the chip is divided into RISC and cryptographic instructions. This provided the user with an option to use the RISC processor for user-defined tasks and also provide cryptographic functions without the need for a separate chip set for security related functions.

The RISC instruction set is comprised of ten basic instruction types. Two instruction types make up the on-chip arithmetic logic unit (ALU): the barrel shifter and multiplier - to perform high speed operations on the data in a bank of 32-bit registers. Three instruction types control the transfer of data between main memory and the register bank. Two instructions control the flow and privilege level of execution, and the remaining commands control and initiate the cryptography to allow the functionality of the instruction set to be extended off-chip in an open and uniform way.

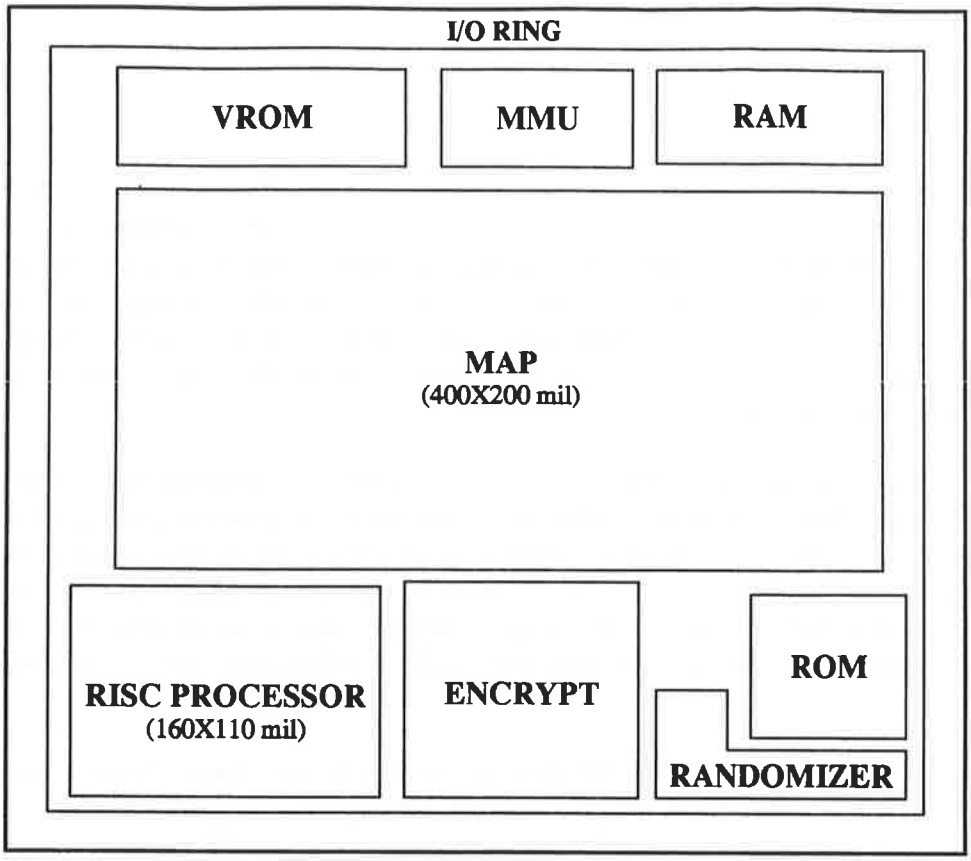
The Capstone instruction set has proved to be a good target for compliers of many different high-level languages. When required for critical code segments, assembly code programming is also straightforward. Capstone is a fully static implementation which allows the clock to be stopped in any part of the cycle with minimal residual power consumption and no loss of state.

CAPSTONE

Offers advanced encryption and authentication technology for digitized voice, data, facsimile, EFT, EDI, and network communications available in a single IC, (MYK-80).

FEATURES:

- **Fully user selectable keys, 2^{80} possible keys**
- **Confidentiality, integrity, and authentication with non-repudiation.**
- **Four cryptographic operating modes (FIPS Pub 81).**
- **On-board non-deterministic randomizer.**
- **Performs Digital Signature & Secure Hash Standard**
- **Message Encryption Key (MEK) generation.**
- **Public Key Exchange (PKE) up to 1024 bits.**
- **Key cover and uncover.**
- **Exportable in products meeting NIST FIPS Pub 140.1 & Government approval.**



CAPSTONE

(499X441 mil.)

RISC	ARM6 32-bit RISC microprocessor, (Apple Newton)
VROM	A one-time programmable Memory (512 X 32 bits)
ROM	Read Only Memory (2048 X 32 bits)
RAM	Random Access Memory (256 X 32 bits)
MMU	Memory Management Unit
MAP	1024-bit Modular Arithmetic Processor
ENCRYPT	SKIPJACK encryption/decryption logic
RANDOMIZER	Digital based non-deterministic noise source

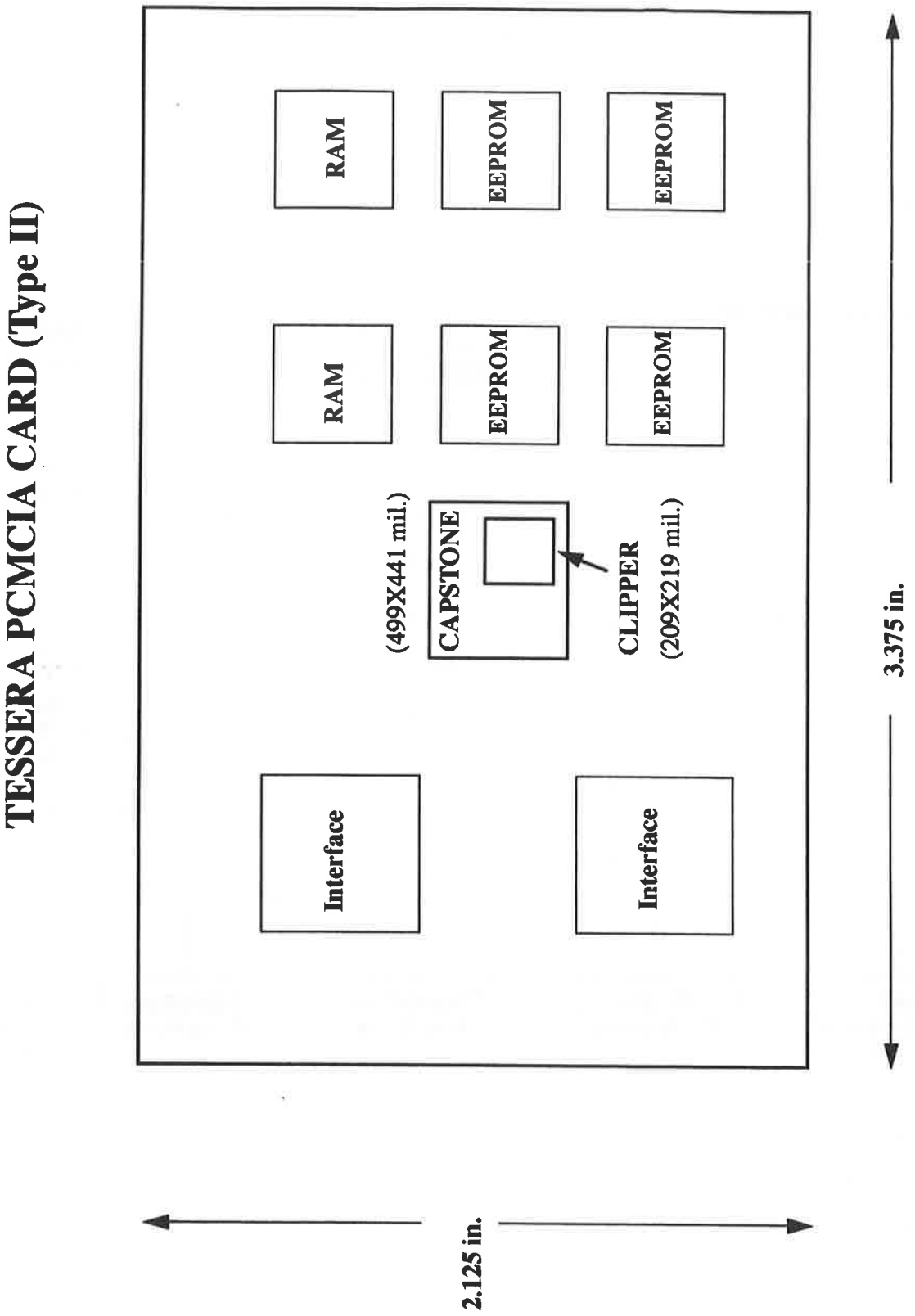
Tessera Description:

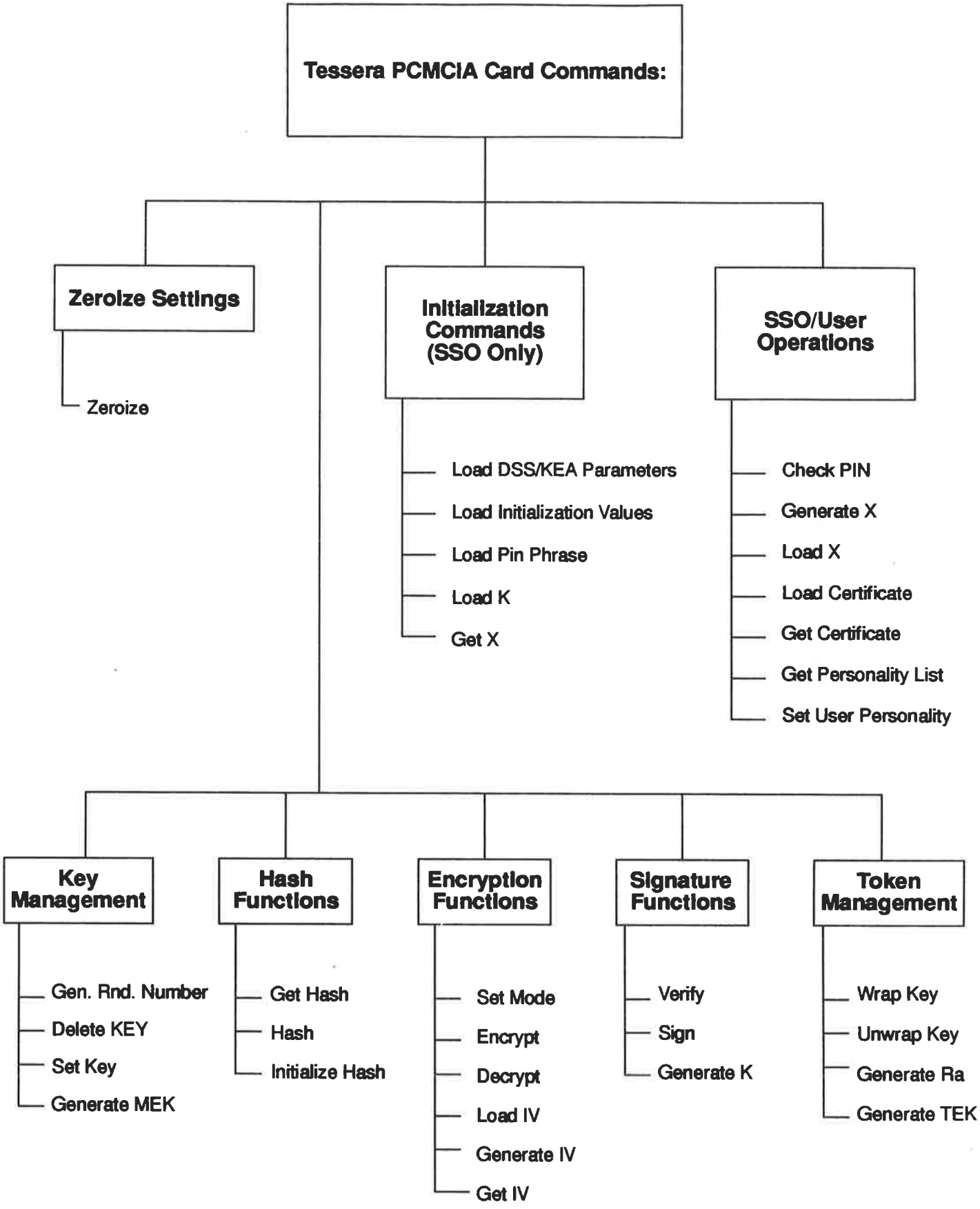
The Tessera Crypto Card is a cryptographic module which implements the Digital Signature Algorithm and the Secure Hash Algorithm of NIST. Additionally, the card supports public/private key exchanges as well as encryption/decryption using the proposed Escrowed Encryption Standard for use in electronic mail and other applications. The card complies with the PCMCIA specification Standard Release 2.0. The card support 35 individual commands which can be used to support cryptographic based authentication and encryption applications.

The Tessera card was designed to provide security for unclassified, highly sensitive electronic mail. The card's cryptographic functions encompass all computer platforms under PCMCIA 2.0 - the cryptographic interface chosen to secure the Defense Message System (DMS), including MILNET and INTERNET. In a single, standardized, easy to integrate cryptographic module, the Tessera Crypto Card provides sophisticated physical security mechanisms and achieves; confidentiality, authentication, data integrity, and non-repudiation.

Based upon the versatile PCMCIA type I card, Tessera's applications encompass many functions well beyond electronic messaging. Among these functions are file and link encryption, authentication, user identification, data integrity, file transfer security, and password generation - to name just a few. Tessera marks the first implementation of the Capstone 32-bit RISC based cryptographic processor, which meets the latest proposed NIST Federal Information Processing Standards (FIPS). Fully DMS compliant, the Tessera Crypto Card features on-board memory and mechanisms needed to generate, store, distribute and control cryptographic keys and user credentials.

Control of the Tessera Crypto Card is provided through a standard C Library command interface or directly through an accessible PCMCIA interface command library. The C Library command interface may be included in the host application program, providing seamless security for each user's application. The Tessera Library provides the application with a platform independent API to the card. This allows the application developer to use a set of ANSI C-compliant function calls to access the card. The device driver provided the library with a platform independent interface to the card. The library communicates with the device driver through the host's file system. Using ANSI standard file streams, the library performs fopen, fclose, fread, fwrite, and fseek commands to send and receive data from the card through the device driver. The device driver makes the card accessible through Centronics, SCSI, Internal (ISA Bus), and Internal Direct Slot PCMCIA adapters.


TESSERA PCMCIA CARD (Type II)
RAM
EEPROM
EEPROM
RAM
EEPROM
EEPROM
(499X441 mil.)
CAPSTONE
CLIPPER
(209X219 mil.)
Interface
Interface
3.375 in.
2.125 in.


Tessera PCMCIA Card Commands:
Zeroize Settings
Zeroize
Initialization Commands (SSO Only)
Load DSS/KEA Parameters
Load Initialization Values
Load Pin Phrase
Load K
Get X
SSO/User Operations
Check PIN
Generate X
Load X
Load Certificate
Get Certificate
Get Personality List
Set User Personality
Key Management
Gen. Rnd. Number
Delete KEY
Set Key
Generate MEK
Hash Functions
Get Hash
Hash
Initialize Hash
Encryption Functions
Set Mode
Encrypt
Decrypt
Load IV
Generate IV
Get IV
Signature Functions
Verify
Sign
Generate K
Token Management
Wrap Key
Unwrap Key
Generate Ra
Generate TEK