



***A smart card operating system built
like a fortress. . .
meant to be attacked***

IBM Research Division Technology Caernarvon Smart Card Operating System

The Caernarvon smart card operating system is a high assurance operating system designed and built with security in mind from the start. It is targeted at Evaluation Assurance Level EAL7, the highest possible level of the Common Criteria, the international standard for evaluating the security components of information systems.¹ High assurance systems like Caernarvon are useful in commercial, government, and military applications, where valuable assets or human lives must be protected from accidents and malicious attacks.

Typical Applications

A Caernarvon smart card should be able to withstand hardware and software attacks, and still function correctly *even when the client system has been compromised*. Examples of security critical functions include providing one end of strong two-party authentication, digitally signing sensitive transactions, protecting and processing confidential data without leaking information, and performing sensitive cryptographic operations that cannot be entrusted to the host client.

Status

A detailed system specification and a preliminary implementation of the system are complete. The cryptographic library has been certified under Common Criteria at EAL5+. Beta testing with customers is expected in 2005.

For more information contact Elaine Palmer, IBM T.J. Watson Research Center, erpalmer@us.ibm.com

Highlights

Supports multiple applications from mutually distrusting (and potentially hostile) sources

High assurance, high security

- targets Common Criteria EAL7
- enforces mandatory access controls
- implements a privacy-protecting authentication protocol
- uses hardware protection mechanisms to enforce security
- ensures integrity of system state across power failures
- cryptographic library certified at EAL5+ (2048-bit RSA, DSA, 3DES, SHA-1, random number generator)

Single, cost-effective, secure card

- field-downloadable applications
- controlled sharing of data between applications
- reduces development and evaluation costs for applications
- potentially limits fiscal liability of card issuer

Portability and Performance

- can host both interpreter-based and native applications (e.g., JavaCard™ and machine language)
- fully compliant with ISO 7816 standards
- defragments memory for efficiency

Strong Authentication

Smart card systems typically leave authentication to application programs, resulting in potential security flaws and inconsistencies in protocols. Caernarvon takes a different approach by providing a very high quality, standardized, cryptographic authentication protocol. It relieves application developers from the task of inventing, designing, implementing, testing, and evaluating their own protocols, thereby reducing development costs. By using a standard protocol, it is easier for a multi-application card to work reliably and securely with applications from many different sources. Authentication is an important component of the operating system that will be covered by the EAL7 evaluation, thus assuring that it actually works and is secure.

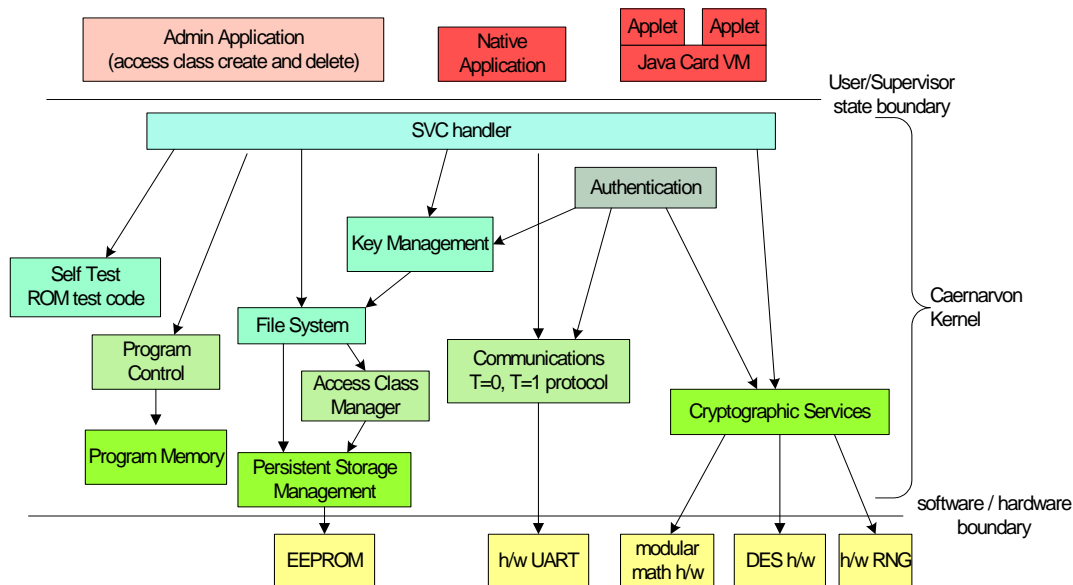
Mandatory Security Policy

The Caernarvon system enforces a mandatory security policy. Each directory or file in the system's storage has an associated *access class*. Access is granted only to those users (programs) that have the appropriate access class, which is determined during the authentication process.

Caernarvon introduces a new approach for multi-organizational mandatory access controls. It provides a mechanism for access controls between different organizations (such as Payroll vs. Purchasing or Department of Defense vs. Department of Energy). This new scheme can handle millions of different organizations with organization-specific security policies, all connected to a common Internet.

Caernarvon has a new approach for defining access classes dynamically in the field. A smart card holder can securely download new applications and access classes from application providers who were not even known to the card issuer at the time the card was issued to the card holder. This feature provides significant benefits, both in commercial applications (where, for example, an airline frequent flier program may sign on new hotel or car rental partners long after issuing a card to a customer) and in the military (where new coalitions may require access by personnel from countries with whom the issuer has never been allied before).

System Architecture



¹ ISO Standards 15408-1, 15408-2, 15408-3, *Information technology - Security techniques - Evaluation criteria for IT security*, International Standard Organization (ISO), 1998-12-18.

TM Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.