

Datacard® Aptura™ Development Card V1.0a (551 851-001)

A simple and stable platform for Java Card™ development

The Datacard® Aptura™ operating system helps make multi-application smart card development simpler and easier and adds greater flexibility and control over the procurement process. The development cards are designed to be used in conjunction with the Aptura™ Applet Development Kit (ADK). The Aptura Applet Development Kit (ADK) contains everything required by a developer to develop, run and test a Java Card™/GlobalPlatform™ applet on an Aptura development card. It is also a good starting point for an issuer's R&D/Technical Department to evaluate the software.

A feature rich Java Card development environment

Aptura Development Card V1.0a is the first version of the Aptura technology, designed for deployment in situations where high quality service provision is essential to business.

The Aptura Development Card V1.0a runs on a Hitachi AE45C chip. The card is identified by the Engineering Part Code (551 851-001).

Aptura™ production chips, equivalent to the development cards, will soon be available. These chips contain the production version of the Aptura operating system.

Aptura portability

The Aptura operating system's 'hardware abstraction layer' helps improve Aptura operating system portability between different chips. This layer acts as a universal 'translator' of the diverse programming interfaces on chips offered by different chip manufacturers.

Improved cryptographic security

The hardware abstraction layer also improves important chip functionality, such as security, by acting as an abstraction layer between hardware and software.

Updateable cryptographic security

The Aptura™ operating system allows security improvements to be made on the card *post issuance* via the Peal™ Proxy application. This facility will be available on future versions of the Aptura development cards and production chips.

On-card debugging

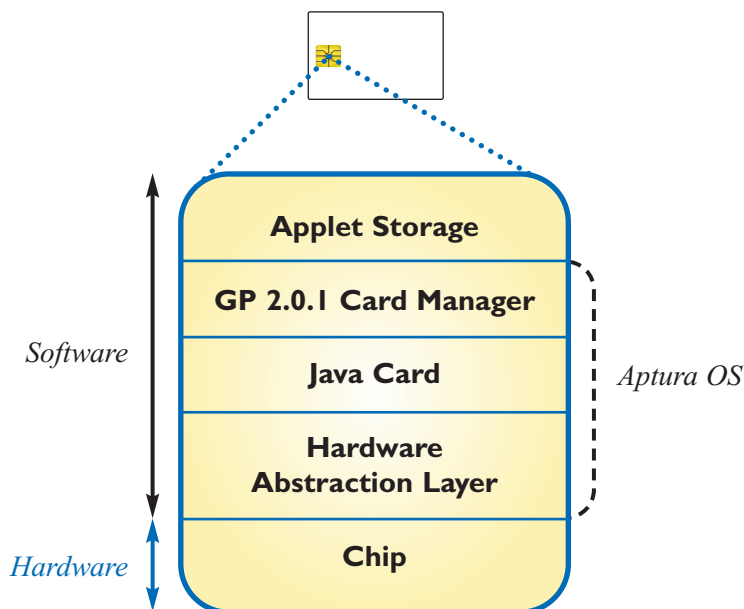
The Aptura development card contains functions not present in the production version that permits source level Java debugging of applets while they are running on the card.

int Data type supported

Unlike many existing Java Cards, the Aptura operating system supports the int data type, a common data type used in application development.

Aptura™ Applet Development Kit (ADK)

The Aptura Development Card V1.0a incorporates an on-card debugger, which can be used in conjunction with the Aptura Applet Development Kit (ADK) and a suitable Java debugger with JDWP to debug and/or test any smart card applications on the card.



Development Card / Production Chip Differences

Development cards and production chips differ in the following ways:

- The development mask contains development keys which are available publicly in Aptura documentation
- The production mask contains production keys which are available only to the issuers
- The development mask contains functional cryptography algorithms
- The production mask contains secure cryptography algorithms
- The development mask contains an on-card debugger within the operating system
- The production mask does not contain an on-card debugger; none of the code is present in the operating system.

In all other aspects, the functionality of equivalent versions/masks of development cards and production chips is identical.

Functional vs. Secure Cryptography Algorithms

It is possible to improve the security algorithms used by the operating system and the applications using the hardware abstraction layer (HAL). Development cards use functional cryptography algorithms with limited HAL protection. Production chips contain further HAL protection, and hence are referred to as secure cryptography algorithms.

Specifications

- Interoperability:
 - Java Card™ compliant:
 - Java Card 2.1.1 Runtime Environment*
 - Java Card 2.1.1 Application Programming Interface*
 - Java Card 2.1.1 Virtual Machine All at Revision 1.0 May 18 2000*
 - GlobalPlatform™ compliant:
 - GlobalPlatform Card Specification Version 2.0.1 7th April 2000*
 - ISO/IEC Standard 7816 compliant
 - All interfaces in Java Card 2.1.1 Application Programming Interface and GlobalPlatform Card Specification are present. However, only those stated as being “supported” will have associated functionality.
- Platform: Hitachi AE45C (HD65145C) smart card chip
- Memory availability: After allocation of Java Card, GlobalPlatform and other system components, available memory is as follows:
 - EEPROM: 32K on chip, 6K for Aptura, 26K available
 - RAM: 4K on chip, 2.4K for Aptura, 1.6K available

Note: The memory available relates to Aptura Development Card V1.0a (551851-001) only and values may differ between equivalent production and development environments. If new applets are required in ROM, please contact Datacard for more details as a new Aptura mask may be required.
- Security evaluation standards: Common Criteria EAL4+ as per ISO/IEC 15408:1999 (pending)
- Implementation Details: The Aptura V1.0a operating system supports:
 - int data type
 - T=0 protocol only
 - Single-, double- and triple-length DES keys. Both types of transient key are supported, as are keys in EEPROM.
 - RSA and RSA/CRT keys of lengths 512, 768 and 1024 bits.
 - ALG_MD5 and ALG_SHA message digest
 - Pseudo random and secure random number generation

- Signature generation and verification with the following algorithms and padding modes, for all key lengths mentioned above:
 - DES_MAC8_NOPAD,
 - DES_MAC8_PKCS5,
 - ALG_RSA_MD5_PKCS1,
 - ALG_RSA_SHA_PKCS1
- Encryption and decryption with the following algorithms and padding modes, for all key lengths mentioned above:
 - ALG_DES_CBC_NOPAD,
 - ALG_DES_CBC_PKCS5,
 - ALG_DES_ECB_NOPAD,
 - ALG_DES_ECB_PKCS5,
 - ALG_RSA_NOPAD,
 - ALG_RSA_PKCS1
- A Global PIN mechanism with support for:
 - Global PIN Management*
 - Global PIN Application Services*
 - Global PIN retry limit and retry counter*
- Security Domain installation
- **The Aptura V1.0a operating system does not support:**
 - Key pair generation
 - Key encryption mechanisms of the Java Card Key Encryption interface
 - Data Authentication Pattern (DAP) verification /Mandatory DAP Verification
 - Delegated Management
 - Velocity checking for repeated application install failure and Card Manager Exceptions. The next version of Aptura (V1.1) will allow developers to implement velocity checking for repeated application install failure and Card Manager Exceptions.
 - Tracing and event logging function

11111 Bren Road West
 Minnetonka, MN 55343-9015
 +1 952 933 1223
 +1 952 931 0418 FAX
 www.datacard.com

Datacard is a registered trademark and service mark of DataCard Corporation. Aptura is a trademark of Datacard Corporation. Java Card is a registered trademark of Sun Microsystems Inc. AE45C is a trademark of Hitachi Ltd.

© 2002 DataCard Corporation. All rights reserved.

Information subject to change without notice.

Printed in U.S.A.

2FL-9004