

Awanee Card Operating System

The WebKomputing Awanee operating system consists of a core Java virtual machine, a class of micro kernels and a series of APIs, which provides the flexibility to rapidly tailor the OS to application requirements and hardware configurations meeting the size, time, power and cost constraints. The product follows the ISO 7816, Java Card™, Global Platform, GSM SIM, CDMA RUIIM, and 3G USIM standards to ensure the application code portable, and applications delivered from different industries interoperable. This capability will allow card issuers to deploy multiple applications via a single card and add value services post issuance. The available APIs will support a wide range of applications from authentication, identification, payment, to loyalty reward, petty cash, ticketing, medical data keeping, IP protection and content access management.

MEMORY REQUIREMENT

It takes 256KB to allocate the complete suite of Awanee operating system, which includes Java Card, GSM, CDMA, GP, VGP, USIM, WIB and other system components. A subset of OS components can be assembled to fit a smaller footprint for a reduced set of specifications.

SPECIFICATIONS

Awanee card operating system complies with:

- ISO 7816
- Java Card 2.2.1
- Global Platform 2.1.1
- VGP 2.1.1
- GSM 11.11, 11.14, 03.19, 03.48
- 3GPP TS 11.11, 11.14, 03.19, 03.48, 21.111, 23.048, 31.101, 31.111, 43.019
- 3GPP2 C.S0023, S.S0053, S.S0078, N.S0003
- SmartTrust WIB 1.2

IMPLEMENTATION DETAILS

Awanee card operating system supports:

- int data type
- Garbage Collection

- T=0, T=1 and T=CL protocols
- Communication speeds up to 115200 baud
- APDU buffer size: 261 bytes
- Generation of RSA and RSA/CRT key pairs of lengths up to 2048 bits depending on coprocessors available
- Velocity checking for repeated application installation failure and Card Manager exceptions
- Single-, double- and triple-length DES keys
- ALG_MD5 and ALG_SHA1 Message digest
- Pseudo Random and Secured Random number generation
- Signature generation and verification with the following algorithms and padding modes:
ALG_DES_MAC4_ISO9797_M1,
ALG_DES_MAC4_ISO9797_M2,
ALG_DES_MAC4_NOPAD,
ALG_DES_MAC4_PKCS5,
ALG_DES_MAC8_ISO9797_M1,
ALG_DES_MAC8_ISO9797_M2,
ALG_DES_MAC8_NOPAD,
ALG_DES_MAC8_PKCS5,
ALG_RSA_MD5_PKCS1,

IMPLEMENTATION DETAILS

(continued)

- Encryption and decryption with the following algorithms and padding modes:
ALG_RSA_SHA_PKCS1
ALG_DES_CBC_ISO9797_M1,
ALG_DES_CBC_ISO9797_M2,
ALG_DES_CBC_NOPAD,
ALG_DES_CBC_PKCS5,
ALG_DES_ECB_ISO9797_M1,
ALG_DES_ECB_ISO9797_M2,
ALG_DES_ECB_NOPAD,
ALG_DES_ECB_PKCS5,
ALG_RSA_NOPAD,ALG_RSA_PKCS1
- A Global PIN mechanism with support for:
 - Management
 - Application Services
 - Retry limit and retry counter
- Security Channel mechanisms through DES encryptions, and digital signatures
- Key encryption mechanisms of the Java Card Key Encryption interface.
- Applet download and delete specified by GlobalPlatform.
- All the APDU commands and file structures required in GSM, CDMA and USIM.
- All the Java SIM classes for STK defined in GSM 03.19.
- OTA and remote file management required by GSM 03.48.
- All the Internet access commands and plug-ins required in WIB 1.2.

SUPPORTED HARDWARE

Awanee COS is currently available in a number of configurations:

- Awanee 100, 200 for Java Card applications on STMicro ST19 & ST21, Philips P8WE, Infineon SLE66, Samsung CalmRISC16 & ARM32, Emosyn TP & TT and EMMicro TCG families.
- Awanee 110, 210 for Java SIM applications on Emosyn TP & TT, STMicro ST 19 & 21, Samsung CalmRISC16, and EMMicro TCG families.
- Awanee 120, 220 for VGP applications on Samsung CalmRISC16 & ARM32, Infineon SLE66 families.
- Awanee 230 for 3G USIM applications on EMMicro TCG, Samsung CalmRISC16 & ARM32 familie

WebKomputing™

650 Castro St., Suite 120-282
Mountain View, CA 94041
Tel: (650) 694-4955
www.webkomputing.com

