

ACOS – Card OS for Industry and Government Applications

ACOS – Operating System Family

- Austria Card's smart card operating system for industry and government applications
- The ACOS core is designed for fast and efficient development of smart card applications
- ACOS has been implemented by Austria Card's research and development team
- All our customers can launch their smart card projects fast and efficiently

Microcontroller Chip

Due to the extensive functionality and the requirement for highest security of Government applications – and in particular for health cards – the chip should be at least a 32K E²PROM chip. This chip features a guaranteed data-retention time of 10 years and more than 500.000 Write/Erase Cycles of the E²PROM.



Cryptography

State-of the art cryptography algorithms are RSA and ECC – Elliptic curves. ECC is preferred due to the higher performance and due to the mathematical model on which the encryption algorithm is based. Cards used in industry and government programmes shall perform the longest possible lifetime. As such, there is no compromise in the length of cryptographic keys. It is possible to handle keys up to 2048 bit.

Certification

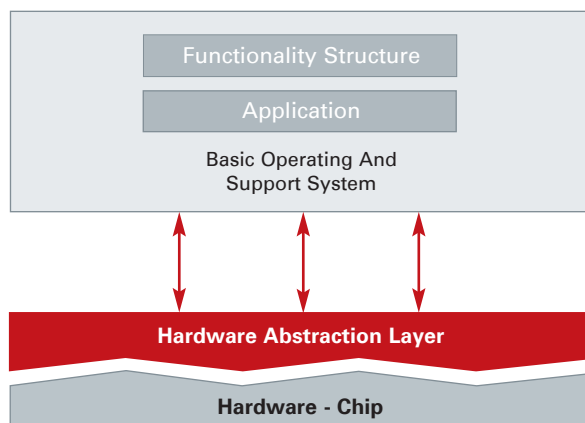
Austria Card's operating system was evaluated according to Common Criteria and received Evaluation Assurance Level EAL 4+, PP conformance: Protection Profile BSI-PP-0006-2002 Secure Signature Creation Device Type 3, V 1.05.

ACOS Features at a Glance

- ☞ Support for multi application cards
- ☞ Smart national ID card functionalities
- ☞ PKI enabled crypto-engine prepared for a certified secure digital signature application
- ☞ Health card functionalities
- ☞ EMV functionalities and electronic purse
- ☞ ISO 7816 compliant smart card operating system
- ☞ Easy and clear file system generation enabled through a file system description tool
- ☞ ECC cryptography with 160 to 256 bit
- ☞ RSA cryptography with 1024 to 2048 bit
- ☞ Fast implementation of cryptographic operations
- ☞ Personalisation solution
- ☞ Protocols T=0, T=1 and T=CL

ACOS Structure - The Need for a Customised Card Operating System

ACOS is based on general market requirements, but its multi-functionality, performance, adaptations and cost-effectiveness are unique in the smart card business. ACOS – as a completely modular system – has combined all hardware related functions in the Hardware Abstraction Layer-HAL.



The HAL enables the operating system to access the memory, communication interfaces, cryptographic coprocessors and further hardware via defined interfaces. Therefore only the HAL has to be updated if an operating system is or has to be transferred to other hardware. Multi-application capabilities of cards allow the different file structures such as health card applications, identification applications, e-Purse or digital signature to work parallel - depending on which kind of commands or applications are requested. The ACOS programming API provides a "C" language interface, which guarantees easy handling, maintenance and reutilisation. The BOSS - Basic Operating and Support System - has a rich functionality framework for the development and building of applications. ACOS is resistant against SPA/DPA and DFA attacks, which has been successfully tested and approved.

Technical data and security aspects

Besides alternative hardware platforms, ACOS is implemented on the Philips P5CC036 microcontroller:

Specification	P5CC036	P5CD036	P5CT072
Contact Interface	ISO 7816	ISO 7816	ISO 7816
Contactless Interface		ISO 14443	ISO 14443
CPU (Bit)	8	8	8
RAM (Byte)	4.608	4.608	4.608
ROM (kByte)	128	160	160
E ² PROM (kByte)	36	36	72
PKI Crypto Engine	FameXE	FameXE	FameXE

Information and Contact

Austria Card GmbH
 A-1230 Vienna | Lamezanstraße 4-8
 T +43 1 610 65-0 | F +43 1 610 65-701
 sales@austriacard.at | www.austriacard.at