OpenCard (Poster Abstract)

Pascal Paillier and Tancrède Lepoint

CryptoExperts, contact@cryptoexperts.com

Smart cards are an opaque technology. Programmable smart cards (JavaCard, MultOS, BasicCard) do not allow access to the (fast!) cryptographic primitive operations on the cryptographic co-processors, and use slow virtual machines. Worse, to access manufactured cards (and their complex software development tools), one has to order high volumes and sign non-disclosure agreements with chip manufacturers.

Introducing OpenCard. OpenCard is a truly, fully *open* smart card that supports user-defined applications developed in native code (C and/or assembly). Its purpose is to provide a simple smart card environment that can serve as a support for instrumenting and testing on-card applications without facing the limitations of cards based on virtual machines. It features a versatile operating system on top of which sets of APDU commands or software extensions containing native APIs, non-volatile data objects and various user-defined customizations are easily installed. Contrarily to other smart card platforms, OpenCard is programmable at a low, close-to-the-hardware level and is 100% user-definable.

Features. OpenCard embeds a 32-bit ARM core (ARM SecurCore SC100), 512kB of flash memory and 18kB of RAM. The operating system provides native access to DES/3DES, AES and RSA co-processors. It also provides an advanced *on-card debugging*: no additional hardware such as emulation boards is required for development. Software development tools are free, open-source and run under Windows, OS X and Unix environments.

Extensions and OpenCard Market. OpenCard makes it easy to program your own cryptographic algorithms and applications making use of co-processors, and even to share your extensions within the OpenCard developers community. An online OpenCard Market displays pre-defined extensions and third-party code that can be easily downloaded into an OpenCard to build up a complete on-card application. OpenCard is ideal for smart card based hardware wallets for crypto-currencies such as Bitcoin.

CryptoExperts. CryptoExperts is a young start-up company founded by internationally recognized industrial and academic researchers in cryptography. Driven by more than 16 years of experience in smart cards development, we are proud to introduce OpenCard. With OpenCard, developers now have deeper access and high flexibility to build innovative, fast and secure smart card applications.

OpenCard will be available by mid 2015, with no minimum order, on
https://www.cryptoexperts.com/opencard