



cv act library/sc – the cryptographic library for smart cards and other security tokens

A cryptovision whitepaper

Version 2.0 (August 2009)

cv cryptovision gmbh

Munscheidstr. 14

45886 Gelsenkirchen

+49-209-167-2477

info@cryptovision.com

With cv act library/sc cryptovision offers a cryptographic library which is especially optimized for the integration of security ICs, just as they are used in smart cards, SIM modules, NFC and USB tokens. On these platforms the library offers an efficient way to realize a complete system with the highest security standards and best performance. Integrated into a smart card operating system, the quality of the cv act library/sc has been proven by several successful evaluations, according to Common Criteria and ITSEC. The library is structured in such a way that it can be used on different microprocessors, while the internal security measures are adapted to specific hardware characteristics. This whitepaper describes the basic functions and architecture of the library.

The cv act library/sc provides a broad spectrum of different routines for the realization of all necessary cryptographic algorithms on smart cards. Integrated into a smart card operating system, cv act library/sc implements the highest security standards with best performance. The main focus is on efficient and particularly secure implementation of public key mechanisms. For this purpose, the cv act library/sc contains all the necessary protocols based on RSA as well as on elliptic curves (ECC) and thus provides the mechanisms of the NSA Suite B or the Extended Access Control (EAC) for machine readable travel documents, for example.

The flexible implementation – with respect to supported key lengths of the public key algorithms and other system parameters like the hash algorithms, for example – ensures that all sorts of security requirements and hardware restrictions can be met. Optimal support of the different hardware platforms leads to the highest performance and security for secret information, e.g. private keys, in existing applications. All routines in the cv act library/sc include state-of-the-art countermeasures against side channel attacks (for example by SPA or DPA, or timing attacks) and fault attacks.

The essential components of the library are implemented in assembly code, in order to provide maximal performance with minimal consumption of resources for the respective destination platform.

The cv act library/sc contains some of the fastest implementations in the industry.

The library is available for processors of the Infineon SLE 66 family, as well as on the NXP P5 platform, with a standard interface which can be integrated into a smart card OS by the customer. Alternatively, both variants can be equipped with a customized interface; if required, the secure integration into a customer OS can be carried out by cryptovision. Additional hardware platforms can be supported on request.

The cv act library/sc is the only product by an independent software producer that achieves usability on different hardware platforms with a standard product. Current applications of the cv act library/sc range from banking, in which millions of licenses for the library have been sold, to ID cards, mobile applications (SIM) and the pay TV sector.

Architecture of the library/sc

The cv act library/sc has a standard API, which accomplishes a simple use of the common cryptographic protocols, and in addition the possibility to utilize basic cryptographic functions to meet even highly specific requirements within a project. The design allows an internal optimization to different microprocessor characteristics, in particular the characteristics of the usual accelerators for long integer arithmetic built into standard smart cards (and security ICs in general).

To achieve this, the library implements an appropriate arithmetic kernel, which itself accesses the internal platform-dependent accelerators for modular arithmetic and basic cryptographic

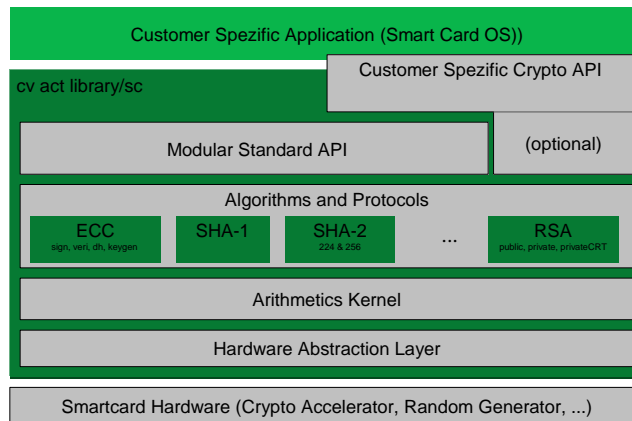
operations via a platform-specific hardware abstraction layer.

For a customer, the use of the cv act library/sc is possible by the modular standard API. In addition, the implementation of a dedicated customer-specific crypto API or an adaptation and direct integration into the smart card OS is possible by request. All components of the cv act library/sc are available as separate modules.

Security measures

Within the layers of the cv act library/sc, different countermeasures are integrated against common attacks such as side channel attacks based on power consumption or electromagnetic radiation by simple or differential power analysis (SPA, DPA), timing or fault attacks.

On the protocol layer these countermeasures are based on appropriate mathematical transformations and arithmetic randomizations. They are complemented by additional hardware-specific countermeasures on the coding level in the lower layers of the library. The implementation of the lower layers is based on the result of intensive examinations of the



cv act library/sc: architecture

characteristics of the respective hardware platforms, in which, for example, security relevant instructions and elementary code fragments are inspected with regard to potential weaknesses.

The complete library is complementarily tested by additional side-channel measurements in an in-house test laboratory. Furthermore, security evaluations of the library were carried out in the context of certifications in independent and internationally recognized laboratories.

Supported algorithms

The cv act library/sc supports signature protocols and encryption with RSA according to PKCS#1 v2.1 and key lengths between 512 (for compatibility with older applications) up to 2048 bits. Since key lengths less than 1024 bits should not be used in up-to-date applications, the RSA key generation is limited to key lengths between 1024 and 2048 bits.

Signatures based on elliptic curve cryptography and based on the field $GF(p)$ – the variant most commonly used today – are possible with ECDSA according to ANSI X9.62 and key lengths between 160 and 521 bits. Other key lengths or variants of the signature protocol (like the variants ECGDSA or ECKDSA) can be supported optionally. In addition, the ECDH key exchange protocol – the elliptic curve variant of the Diffie-Hellman protocol - according to ANSI X9.63 is available.

The implemented hash functions are SHA-224, SHA-256 and due to compatibility reasons SHA-1, all according to FIPS 180-2. The symmetric encryption algorithms AES (according to FIPS 197), DES and Triple-DES (according to FIPS 46-3) are optionally available.

Additional mechanisms are integrated for the creation, processing and validation of random numbers according to AIS 20 and AIS 31. To achieve higher efficiency, different kinds of random sources are used internally, depending on the type of application (for instance algorithmic randomizations on the one hand, or key generation with a high entropy demand on the other hand).

All implementations follow internationally accredited standards. The integration of additional algorithms and protocols like DSA, different symmetric ciphers or supplemental hash functions are possible on request.

Evaluation according to ITSEC und Common Criteria

The cv act library/sc is a standard product, which is the result of a continuous enhancement process and which is used by millions of end-customers –

integrated in the smart card operating systems of different vendors. As an integral part of these operating systems, the cv act library/sc has passed various evaluation and certification processes according to Common Criteria (CC) and ITSEC. The corresponding certificates (CC EAL 4+, ITSEC E4/high) attest to the quality and the high security level of the implementation. As part of a customer project, complete support of the evaluation process, including the compilation of the appropriate evaluation documents, is also possible as a service.

The continuous maintenance of the product ensures that the supported algorithms and their implementation remain state-of-the-art. A parallel development on different hardware platforms or a subsequent platform change is made easier, thanks to the multi-platform architecture. A further advantage of the cv act library/sc, compared with other cryptographic implementations that are sometimes directly available from the semiconductor manufacturer, is the availability on different microprocessors and its expert evaluation and integration support.

Additional services

Beyond the cv act library/sc, cryptovision offers the customized implementation or adaptation of implementations on smart cards and security tokens. Further, comprehensive services for quality assurance of existing implementations in the in-house side-channel laboratory and project-specific security consulting are also offered.

The cryptography know-how of cryptovision is also available in the form of bulk produced smart cards, in fact as Java cards as well as classical smart cards with an ISO 7816-4 interface. It is self-evident that these cards support – besides the RSA standard – also protocols based on elliptic curves. More information is available on request.

Complementing the cv act library/sc, cryptovision offers additional cryptographic libraries within its cross-platform concept, ranging from VHDL modules, a library for embedded systems processors, to a library for workstations and servers with support for

smart cards, security tokens and Hardware Security Modules (HSM). In addition, customized components are obtainable on demand.