



cv act library/es – the Cryptographic Library for Embedded Systems

A cryptovision whitepaper

Version 1.0 (August 2009)

cv cryptovision gmbh
Munscheidstr. 14
45886 Gelsenkirchen

+49-209-167-2477
info@cryptovision.com

With cv act library/es, cryptovision offers a flexible and efficient way for realizing security-relevant functions in embedded systems, e.g. in automotive electronic control units, point-of-sale terminals or measuring systems, with cryptographic mechanisms. The product is optimized for minimal resource consumption, nonetheless delivers high performance on a wide range of hardware platforms. This whitepaper describes the basic functions of the library, typical fields of application and the option to use the freely available performance evaluation tool (PET) for cv act library/es to evaluate possible applications of cryptographic mechanisms and the performance achievable on actual hardware platforms.

Cryptographic securing processes play an increasingly important role in the embedded systems sector. Typical application scenarios are the protection of software integrity within the flash update of automotive ECUs, the encryption of communication links and the prevention of fraudulent use in point-of-sale terminals. Apart from these conventional applications, cryptography allows for entirely new forms of value creation, including activation of chargeable software and content, Pay-TV or various other applications. In addition, digital signatures provide means to protect the integrity of metered values and other pieces of data, e.g. gas or power consumption data.

To realize those mechanisms, an especially optimized software library for embedded systems is necessary, which is usable on the numerous different microcontrollers used in this field and which realizes the relevant security functions.

The cv act library/es

The cv act library/es is a cryptographic library especially tailored to be utilized in embedded systems. It has a ANSI-C interface and offers all mechanisms to guarantee confidentiality and authenticity of transferred or stored data. This includes symmetric encryption algorithms, public key algorithms for digital signature generation and cryptographic key exchange, hash functions and

secure random number generator. All algorithms are implemented to be used in embedded system applications and are optimized for the processors used in this sector. The flexibility of the implementation ensures that the requirements of various applications are met, with regards to security needs and operational environments, while the solution complies with well-established cryptographic standards.

The modular design of cv act library/es permits easy adaptation to various hardware platforms. The interface and internal structure allow for memory, security and time-critical parts to be optimized – if necessary using assembly code – according to the customer’s needs.

The cv act library/es is available for virtually any processor typically used within embedded systems. Ranging from 8 bit processors like the Atmel AVR or processors based on 8051 cores, 16 bit processors like the Motorola HC12 to various MIPS, ARM and PowerPC-based 32 bit processors. Indeed, use on standard 32-bit PC processors is also possible. Thus, the

spectrum ranges from high-end platforms down to processors designed for minimal power consumption (such as the MSP 430 from Texas Instruments), which are all capable of strong asymmetric cryptography with cv act library/sc.

Versions for hardware platforms that are not supported by the standard version of cv act library/es can be realized quickly. The library is already used in applications on more than a dozen different processors, and the number of supported hardware platforms is always increasing.

Technical specifications and information about memory footprint, stack size, RAM consumption and performance are all available on request. If you wish to see timings for cryptographic operations on your specific hardware platform, you can apply the performance estimation tool (PET) for the cv act library/es.

The Performance Estimation Tool (PET)

The performance estimation tool is an independent software tool that is distributed by cryptovision on demand. It permits the estimation of expected calculation times of cryptographic operations on an arbitrary hardware platform. The only constraint is the availability of an ANSI-C compiler for the processor in question; porting the performance estimation tool is easy and it is adequately documented.

The performance estimation tool measures the specific timing of basic operations on the hardware. After transfer of the data to cryptovision and subsequent analysis, the

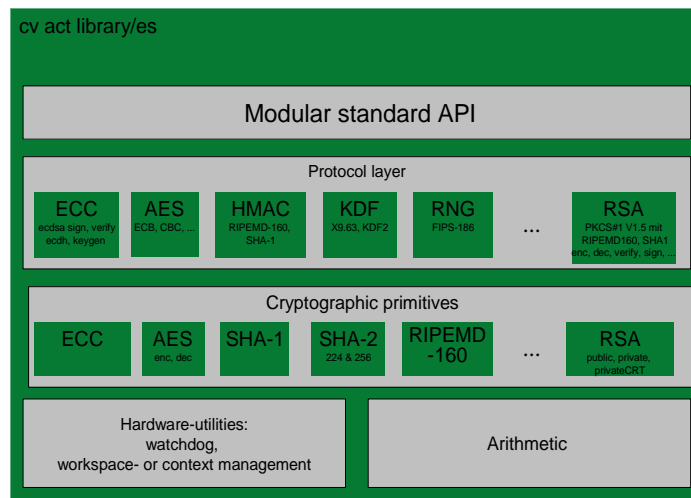
results are given back without obligation and free of charge.

More information can be found at www.cryptovision.com/pet.

Architecture of cv act library/es

The architecture of cv act library/es profits from the experience cryptovision has gained implementing cryptographic mechanisms on smart cards and other high-security platforms.

The library has a standard API that allows simple usage of most common cryptographic standard



cv act library/es: architecture

protocols (e.g. an AES with CBC block mode). To allow realization of specific project requirements, additional basic cryptographic functions (e.g. the basic AES operation on a single block) can be used directly. The design accomplishes an easy adaptation to different processor characteristics, such as word size or the size of the internal multiplier.

Watchdog calls are supported and guarantee a continuous control by the application above.

Product features

The cv act library/es was developed to meet the highest standards in terms of portability in ANSI-C, with special respect to the MISRA directives.

The user of the cv act library/es gets a standard product which is maintained and refined continuously, and which is currently in the field in hundreds of thousands of different devices. Examples are complex measuring systems, navigational devices (GPS) and the electronic control units of several well-known German car manufacturers.

A continuous maintenance and product enhancement process ensures that the supported algorithms and their implementation stay state-of-the-art. Subsequent platform changes by a customer present no technical problems. cryptovision assures that the cv act library/es can be used on any new processor platform without significant code changes.

Asymmetric algorithms like RSA – important for digital signatures and key exchange – as well as elliptic curve cryptography (ECC) are supported. ECC is the basis of many modern applications; thus, the cv act library/es provides the mechanisms of the NSA Suite B and the Extended Access Control for machine readable travel documents, for example.

Performance of cv act library/es

The cv act library/es features a very small footprint together with impressive calculation times. It gives application support for asymmetric and symmetric cryptography, with hash and random number generation typically needing less than 16kb for the cryptographic routines. If an integration of minimal

functions is necessary, the footprint is diminished correspondingly. More precise numbers can be given once an analysis with the performance estimation tool has been carried out.

In addition to the standard ANSI-C variant of the product, a customer-specific, platform-dependent adaptation is possible, where parts of the code are optimized by assembly code modules. In this case optimizations by a factor of 2-3 are possible; exact numbers vary from platform to platform.

Additional services

As well as cv act library/es, cryptovision offers additional project support and consulting. This ranges from the preparation of security concepts and workshops on secure deployment of cryptographic functions to custom development and assistance with the installation of a complete system, including infrastructure components for key and certificate management.

Complementing the cv act library/es, cryptovision offers additional cryptographic libraries within its cross-platform concept, ranging from VHDL modules, a library for different smart card 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 available on request.

Complementing the cv act library/pc, cryptovision offers additional cryptographic libraries within its cross-platform concept, ranging from VHDL modules, a library for different smart card processors, to a library for 8-, 16- or 32-bit embedded processors. In addition, customized components are available on request.