



# cv act library/pc – the cryptographic library with smart card support

## 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/pc, cryptovision offers a modular C++ library for the development of security-relevant applications. Possible fields of application range from adding security functions to an existing software solution to implementing fully fledged security software. As an example, the cv act library is used for the German electronic passport border control systems. The library contains all prevalent cryptographic algorithms and allows for easy integration of smart cards, other security tokens and Hardware Security Modules (HSM). This whitepaper provides an overview of the functional scope and the employment of the cv act library/pc.

Protecting the confidentiality and integrity of data as well as its liability and authorship is a central concern in a lot of IT applications. These requirements can be fulfilled by cryptographic mechanisms providing authentication, encryption and digital signatures.

Often these security functions cannot be realized with the aid of off-the-shelf application software, since it either does not meet the security demands or cannot successfully be integrated into the existing software and process environment. In such cases a custom development is preferable. Using a purpose-build library reduces the implementation effort and the risk of errors in the realization of the often rather complex cryptographic functions.

### **The cv act *library/pc***

The cv act *library/pc* is a cryptographic library optimized for use on standard PC platforms. It provides a flexible, object-oriented C++ interface and contains everything needed to develop security-relevant applications. This comprises asymmetric ciphers, challenge & response protocols, mechanisms for digital signatures including the necessary hash functions, random number generators and functions for the generation, exchange and derivation of cryptographic keys. The functional scope of the cv act library/pc provides all prevalent cryptographic algorithms, in particular those approved by the German electronic signature act as well those defined by the NSA within its Suite

B initiative. Moreover the cv act library/pc is adapted for realizing Extended Access Control (EAC) mechanisms, based on Elliptic Curve Cryptography (ECC) and used for the German electronic passport.

All cryptographic algorithms comply with, and are tested against, the relevant standards (ANSI, ISO/IEC and IEEE) to guarantee the maximum possible interoperability.

### Product features

With cv act library/pc one obtains a standard product that is subject to continuous enhancement and has been used successfully in numerous applications for years.

The continuous maintenance of the product guarantees that all cryptographic algorithms are always kept state-of-the-art. A change of the customer's hardware platform is also always possible.

The flexible implementation meets the demands of a variety of applications, in terms of security and application environments. The cv act library/pc is prepared to be used with special security hardware: smart cards, other security tokens and Hardware Security Modules (HSM) can all be integrated via unitized mechanisms using standardized interfaces (CSP, PKCS#11). Such security hardware can be used to securely store private keys, for example. It even allows the generation of keys and performing the corresponding cryptographic operations directly on the hardware device itself, so that private keys never leave the protected environment.

### Architecture of the cv act library/pc

The cv act library/pc was designed in accordance with the principles of object-oriented software development and complies with the ISO/IEC 14882

standard. The following figure depicts an architectural overview.

Using a modular approach, the cryptographic algorithms and protocols are separated from the

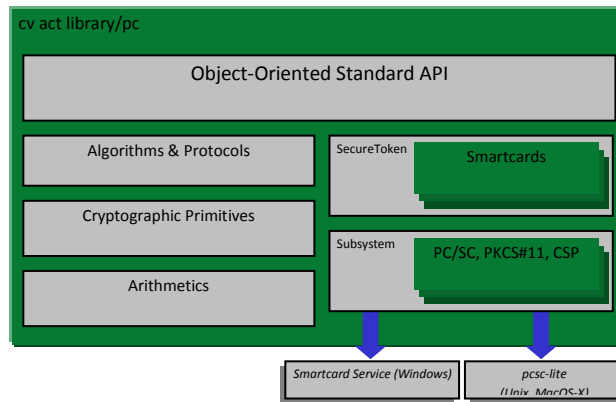
underlying cryptographic primitives, which in turn are separated from the basic long-integer arithmetic.

This not only makes the code independent from the particular algorithm used, but also from the principal mechanism at large.

Moreover, it allows for integrating additional cryptographic algorithms, so that the higher-level protocols can use them directly.

As an example, hardware random number generators can easily be integrated and used for key generation without any modifications to the respective routines.

All included cryptographic functions are called using a unitized interface.



cv act library/pc: architecture

### References

The development of the cv act library/pc benefits from cryptovisions experience in the smart card and high security areas. The following sample projects all use the cv act library/pc as their cryptographic foundation and illustrate the high security level it provides:

- cv act s/mail: All internal cryptographic functions of this email security plug-in are based on the cv act library/pc. This email plug-in has successfully passed all the interoperability tests performed by the German Federal Office for Information Security (BSI) within the SPHINX initiative. It is approved for information classified "NATO RESTRICTED" and "VS-NfD" (official use only) according to German federal law. cv act s/mail is officially recommended by the NATO.

- MediaTrust: Electronic billing

Within the MediaTrust solution for electronic billing, the verification component, based on the cv act library/pc, has been evaluated and certified according to “ITSEC E2 (high)”.

As well as employing cv act library/pc for internal products, it is also used in the following products:

- Reference software for interoperability testing of electronic passports (“Golden Reader Tool”, GRT):

The Golden Reader Tool was developed by the BSI to validate the security functionality of various international implementations of the Machine Readable Travel Documents (MRDT) standard. In this tool, the cv act library/pc is used for all cryptographic operations as well as for certificate management; this comprises, among other things, signatures based on the Elliptic Curve Digital Signature Algorithm (ECDSA) as used for the “Extended Access Control” mechanism.

- Border control systems for electronic passports:

The German “Bundesdruckerei” uses the cv act *library/pc* in mobile systems for electronic passport verification. This application also incorporates mechanisms based on elliptic curves.

library for 8-, 16- or 32-bit embedded processors. In addition, customized components are available on request.

## ***Additional services***

Further to this cryptographic library, cryptovision offers additional project support and consulting. This ranges from the preparation of security concepts, workshops on secure deployment of cryptographic functions, custom development and assistance with evaluation/certification according to international IT security standards such as ITSEC or Common Criteria, to the installation of a complete system including the infrastructure components for key and certificate management.

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