



Infrastructure Components for Electronic ID Applications

A cryptovision whitepaper

Version 1.0

cv cryptovision GmbH
Munscheidstr. 14
45886 Gelsenkirchen

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

Electronic ID documents provide advanced security and allow for various additional applications. Besides an e-ID public key infrastructure, additional software components are necessary to implement the security mechanisms in the infrastructure, for instance within inspection systems. Cryptovision provides an approved set of state-of-the-art software libraries to integrate the security mechanisms in inspection and background systems.

Implementing an e-ID infrastructure

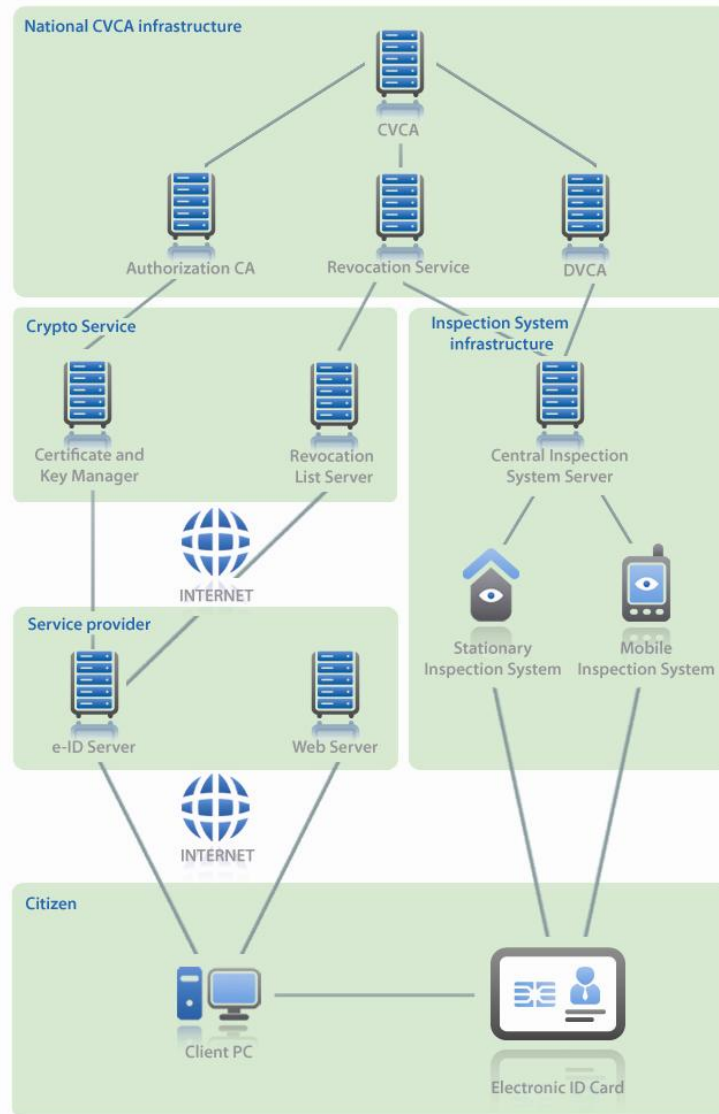
Electronic Machine Readable Travel documents (MRTD) and electronic (citizen) ID documents are widely used worldwide. They provide enhanced security due to an embedded – commonly contactless – security chip that stores the holder’s personal information and additional biometric data. The chip’s processing capabilities allow for effective access control to this information based on strong cryptographic mechanisms, including chip and terminal authentication and encrypted data transfer.

For the realization of the security mechanisms in the corresponding infrastructure components, cryptovision offers a complete set of software libraries and consulting services. With the help of these libraries, customers can easily integrate their

own security applications saving development time and minimizing project risks.

An e-ID infrastructure typically consists of different security-relevant systems. With cryptovision, the security mechanisms can be implemented with one homogeneous tool set independent of the hardware platform and operation system, regardless if inspection systems or service providers have to be realized.

This whitepaper focuses on the tool chain for devices and their integration into an e-ID infrastructure. Additionally, cryptovision provides full e-ID capable PKI solutions, middleware and Java Card applets for e-ID cards. For more information about this components please refer to the respective whitepapers available at www.cryptovision.com.



Scheme of an eID infrastructure: eID documents provide electronic holder identification with dedicated inspection systems, but also authentication for a variety of private sector applications and web-services. In the latter case, crypto service providers fill the gap between the national infrastructure and the service provider.

Inspection systems

Electronic passports following the MRTD standard are designed to be verified by dedicated inspection systems, reading the machine-readable zone of the passport and initiating a cryptographically secured data exchange between passport and inspection system. A typical use case is border control. Mobile inspection systems are typically based on embedded

computers with a Windows CE, Linux or proprietary operation system. Stationary inspection systems are sometimes also implemented based on standard PC architectures.

Service providers

Beyond the original sovereign application, e-ID documents often implement more advanced security mechanisms that can additionally be used for

interesting governmental and private sector applications. This covers authentication at web portals and electronic services, age verification, qualified electronic signatures for legally binding transactions, electronic ticketing & payment and much more. While the basic MRTD security mechanisms are standardized, these additional functions and the cryptographic mechanisms employed differ widely in different projects.

As outlined above, the platforms to be supported in an e-ID infrastructure are manifold: they can vary from workstations and servers with standard PC operation systems down to mobile border control systems based on embedded systems with Windows CE or Mobile, as well as other operation systems.

Solutions for e-ID infrastructure

Depending on the target platform, cryptovision offers three different cryptographic libraries: a library optimized for servers, workstations and larger embedded devices based on Windows mobile or Windows CE, a library optimized for smaller embedded devices and a library for security ICs used in smart cards or other devices. With these libraries, all cryptographic services can be implemented with a consistent tool set.

In case of special project requirements, all libraries can be customized and extended with specific security mechanisms and protocols.

In addition, cryptovision provides a wide range of further products for e-ID applications, ranging from Java Card applets for e-ID security mechanisms, smart card middleware to a complete e-ID capable PKI solution.

Complementing the software products, cryptovision offers comprehensive project-specific security consulting and services, starting with the specification of the system and including the complete integration of the security services within a customer project. For quality assurance of existing e-ID and MRTD implementations, cryptovision can rely on an experienced in-house side-channel laboratory.

The highly qualified consultancy services we provide underpin the effective integration of our security products. After successfully completing many major projects, our consultants possess a profound theoretical and practical expertise, further sharpened by close collaboration with product development. Our consultancy service spectrum ranges from the risk analysis of subsystems or standalone systems, the design of complete cross-platform security architectures to the support or full service for evaluations and certifications according to official IT security standards like common criteria and others.

The components in detail

The cv act library/pc

The **cv act library/pc** is a cryptographic library optimized for Windows (including Windows CE), Linux, MacOS or Solaris platforms. It provides a flexible, object-oriented interface and contains all cryptographic mechanisms needed to implement e-ID and MRTD security mechanisms and other security-relevant applications.

This comprises asymmetric ciphers, challenge & response protocols, mechanisms for digital signatures including the necessary hash functions, random number generators, functions for the generation, exchange and derivation of cryptographic keys and for the handling of digital certificates. All cryptographic algorithms comply with, and are tested against, the relevant standards (ANSI, ISO/IEC and IEEE) to guarantee the maximum possible interoperability. This assures that existing and future cryptographic mechanisms can be implemented.

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. Thus, crypto service providers in e-ID applications can easily rely on trusted security hardware, for instance if smartcards

are used to distribute and store authorization certificates.

The **cv act library/pc** is a sophisticated product, used within the reference software for interoperability testing of electronic passports (Golden Reader Tool) and also providing the cryptography within German inspection systems.

Thus, the application area of the **cv act library/pc** ranges from (mobile) inspection systems – for instance, for border control – and stationary inspection systems to larger infrastructure components for crypto service providers.

The **cv act library/es**

If mobile components – for instance for inspection systems – have only limited processing performance, the **cv act library/es** provides the cryptographic mechanisms. It is a cryptographic library especially tailored to be used in embedded systems. The **cv act library/es** has an ANSI-C interface and offers symmetric encryption algorithms, public key algorithms for digital signature generation and cryptographic key exchange, hash functions and a secure random number generator.

The **cv act library/es** is available for virtually any processor typically used within embedded systems, and can especially be used to implement compact and energy-efficient systems based on any hardware and operation system.

The **cv act library/sc**

cv act library/sc provides a broad spectrum of different routines for the realization of all necessary cryptographic algorithms on security ICs, just as they are used in smart cards, SIM modules, NFC or USB tokens, and e-ID or ePass systems. Integrated in a smart card operating system, the **cv act library/sc** accomplishes the highest security standards with best performance.

In many cases cryptovision libraries are a part of components which were high level certified along standards like common criteria or others.

Integrating cryptovision's libraries

The cryptographic libraries of cryptovision are delivered as object code with an easy-to-use interface. The large variety of different supported algorithms and cryptographic protocols allows the support of even exotic security mechanisms.

On request, cryptovision provides training and consulting as well as tools and support for the realization of the cryptographic services. The **cv act library/es** is designed to be compiled exactly for the customer's combination of processor, compiler and development environment. Non-standard security mechanisms can easily be added.

Conclusion

The cryptographic libraries of cryptovision are especially suited to implement e-ID inspection systems and security mechanisms for crypto service providers. They provide secure and efficient implementations of all necessary cryptographic mechanisms in a ready-to-use package. With the help of these libraries, customers can easily integrate their own security applications saving development time and minimizing project risks.

Additional solutions and services

In addition to the cryptographic libraries, cryptovision offers software products to set up and secure MRTD and e-ID applications.

cryptovision's e-ID Java card applets

cryptovision provides a set of Java Card applets for electronic ID documents and ICAO-compliant machine readable travel documents (MRTD). Applets are available for Basic Access Control, Extended Access Control as well as for added-value applications like digital signatures or encryption.

Public Key Infrastructure

cv act PKIntegrated is a sophisticated software solution for generating certificates and managing their lifecycle. It supports an extensible variety of certificate formats, smart cards, certificate

revocation lists, online certificate validation via OSCP, certificate registration via SCEP and a range of cryptographic methods and key lengths. With its comprehensive support for elliptic curve cryptography (ECC) it is ideally suited for EAC infrastructures.

Smart card middleware

With **cv act *sc/interface***, cryptovision offers a seamlessly integrated middleware for smart cards and security tokens like e-ID cards. **cv act *sc/interface*** runs on several platforms (Windows, Windows Mobile, Mac OS X, Linux). Because **cv act *sc/interface*** implements the PKCS #11 standard and includes a Microsoft Cryptographic Service Provider (CSP) as well as its own mini-driver, it can be integrated into nearly every application including Web browsers. **cv act *sc/interface*** is the first smart card middleware that supports ECC algorithms with a key length up to 521 bit. Additionally it is also possible to replace the PIN with a biometric trait, e.g. a fingerprint. Via the Match-on-Card Technology it is assured that sensitive data like a fingerprint is saved on a smart card and not on a PC.

cryptovision

cryptovision is a leading supplier of innovative IT security solutions based on cryptography. The company specializes in lean add-on components, which can be integrated into nearly any IT system to gain more security in a convenient and cost effective way. Based on its 10 year market experience and broad background in modern cryptography – such as ECC (elliptic curve cryptography) – all cryptovision products continue to provide the most state-of-the-art and future-proof technologies. From small devices like citizen e-ID cards up to large scale IT infrastructures, more than 30 million people worldwide make use of cryptovision products in defense, automotive, financial, government, retail and industry.

References

For more details about the cryptographic core components of cryptovision please refer to: www.cryptovision.com.