



Combining Physical and Logical Access

A cryptovision whitepaper

Version 1.0

cv cryptovision GmbH
Munscheidstr. 14
45886 Gelsenkirchen

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

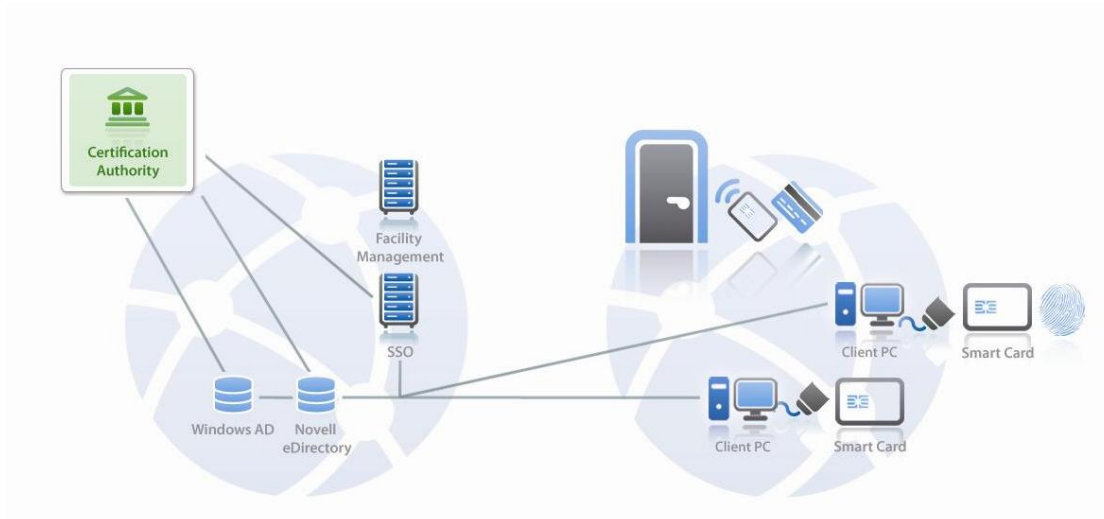
*If user accounts in physical and logical access systems are managed in the same system, this increases security and helps to decrease administration effort. In addition, such a solution offers several options for advanced monitoring and helps to detect account theft. This paper shows, how physical and logical access can be combined using the cryptovision products **cv act sc/interface** and **cv act PKIntegrated**.*

Protecting enterprise values is a core task of logical and physical security departments. In a time of decreasing budgets and technological overlaps both departments face increasing pressure for convergence of both fractions. Communication between logical and physical security staffs is not always peaceful, although they have similar goals – protecting a company’s most important values.

In 2008 a major study project detected increasing spendings on mergers of logical and physical access control systems (both, private and public sectors were covered). The study assumes that the expenses will increase tenfold within the next three years. Several programs and legislative initiatives, like the Homeland Security Presidential Directive 12 in the U.S., suggest healthy growth in the future.

Therefore, CIOs are facing increasing requests for budgetary plans for new access control systems which includes new hardware for every user, identity management software and per user authentication credentials they have to legitimate to their CEOs and CFOs. In addition there are efforts necessary for end user training and IT-helpdesk. Such overlapping brings the changes in technology on display. An increasing number of requirements originated in physical access lead to installations depending on company ID cards, computer networks, and software-based access policies. All of these are core competence of IT departments.

Alliance of physical and logical access



Protection of physical and logical access can be implemented with the same card. For logical access, usually digital certificates (provided by a Certification Authority) are used.

When logical and physical access are combined, it is a core requirement that one single company ID-card is used for both purposes. Physical access is usually implemented with a low-end contactless chip, while logical access is based on digital certificates. A digital certificate can be thought of as a digital passport that is issued to a person. Smart cards with two chips (or dual interface cards) are used to meet the requirements of both, physical and logical access solutions. Most card manufacturers provide applicable smart cards in their standard portfolio. In order to manage digital certificates, a special component (Public Key Infrastructure) is necessary. A Public Key Infrastructure (PKI) is responsible for issuing, exchanging and revoking digital certificates.

With his combined card, the user enters the company building in the morning and uses his ID card to open the door to his office. Afterwards he logs into the internal network with the smart card part of his ID card. If he leaves his desk, he removes the smart card out of the smart card reader and the screen is locked. Upon returning to his desk he authenticates again and continues his work.

Any sort of event within this system is subject to monitoring (e. g. someone logs into the network twice/with two computers, someone enters the building together with another employee without

presenting his ID card and logs into the network by smart card afterwards).

Of course, combining physical and logical access requires more than only merging two card models. In fact, the task goes beyond technology – involving also business processes and even establishing a new process for identity validation. A company card is almost useless if the identity of the owner is not verified.

It is most advisable that companies facing such a challenge break the big picture into smaller ones. It is most likely to divide such a project into the following subsets:

- One single company ID-card for logical and physical access
- Centralized management for ID-cards instead of several different user databases
- One step enrollment and termination/revocation of a user and his ID card (provisioning) Single-step user/card enrollment (provisioning) in all databases for access control and identity
- Unified event correlation: Such a system is designed to alert you when Mary logged into the wireless network (an event that occurs in the logical access control system), but she didn't enter the building (source of this event: physical

control system). It's rather likely that someone hijacked Mary's wireless account.

cryptovision's solution

When using digital certificates on smart cards, a smart card middleware implements the connection between the application and the card. A powerful smart card middleware not only enables access to the digital certificate on the card, but it also provides additional functions for formatting, PIN change, PIN unblocking and others.

The cryptovision product **cv act sc/interface** is one of the most powerful on the market. It runs on several platforms (Windows, Windows Mobile, Mac OS X, Linux) and supports all relevant standard interfaces for smart card access. 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 also provides the PKI solution **cv act PKIntegrated** with highly sophisticated certificate management abilities, which covers the whole lifecycle of a digital certificate (certificate lifecycle management). **cv act PKIntegrated** 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.

In contrast to almost any other CA solution, **cv act PKIntegrated** was from the beginning not designed as stand-alone component, but as an add-on to user management systems. This is a considerable benefit, because the registration of new users, the change of user attributes, and the deletion of user entries can

be easily connected with certificate creation, certificate change and certificate revocation.

In addition to managing certificates, it is important for an enterprise to have an overview on all existing smart cards. In small environments, this can be achieved manually, but as the amount of smart cards increases, it gets more and more important to use a card management system (CMS). A CMS supports card formatting, card application control, card revocation and other processes. In addition, a CMS can be connected to a smart card personalizing machine, which facilitates the personalization process considerably.

cv act PKIntegrated interoperates with several different card management systems. For typical enterprise requirements, cryptovision offers its own product **cv act card/manager**. As it is integrated into user managements systems in the same way as **cv act PKIntegrated**, it interoperates perfectly with **cv act PKIntegrated** and **cv act sc/interface**. However, at least half a dozen other CMS products can be used, including the high-end solutions A.E.T. BlueX, ActivIdentity Card Manager, Secude TrustManager, and VPS IDExpert.

If **cv act PKIntegrated** and **cv act card/manager** are jointly used, integrate processes are possible. In case of termination of an employment the ID card is revoked by an administrator or an employee from the HR department. This revocation is entered just once, e. g. in the company's HR application. Afterwards this new status is transferred automatically to the physical control system, the enterprise authentication service and to the PKI. Straight after the revocation of the ID card it isn't possible any more to enter the company's building or to log into the company's internal network. The credentials of the user are no longer valid for either application.

There are additional advantages of the integrated approach of **cv act PKIntegrated**: it neither needs a user interface of its own nor a database nor additional protection, because all this is provided by the identity management system. **cv act**

PKIntegrated is therefore a very lean and cost-effective solution.

Many customers use **cv act PKIntegrated** with the Novell Identity Management suite. There is a seamless integration of **cv act PKIntegrated** into the Novell eDirectory and the Novell Identity Manager (these two components are the core of the Novell Identity Management portfolio). However, **cv act PKIntegrated** also interoperates well with other identity management solutions, for instance with the Oracle Identity Management and the IBM Tivoli Identity Manager.

Conclusion

Logical and physical access should be combined and should result in one company ID card. Such ID card is used for access to company's buildings and serves also as a smart card for network login. This is the basis for a background system that decreases the effort for user administration tremendously. With one click a user account can be created or terminated.

cv act sc/interface serves as a key component in this process to assure the connection between company ID card and computer. **cv act PKIntegrated** and **cv act card/manager** are used for the management of the cards and the digital certificates.

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 cryptovision's products refer to: www.cryptovision.com.