



Strong Authentication

A cryptovision whitepaper

Version 1.0

cv cryptovision GmbH
Munscheidstr. 14
45886 Gelsenkirchen

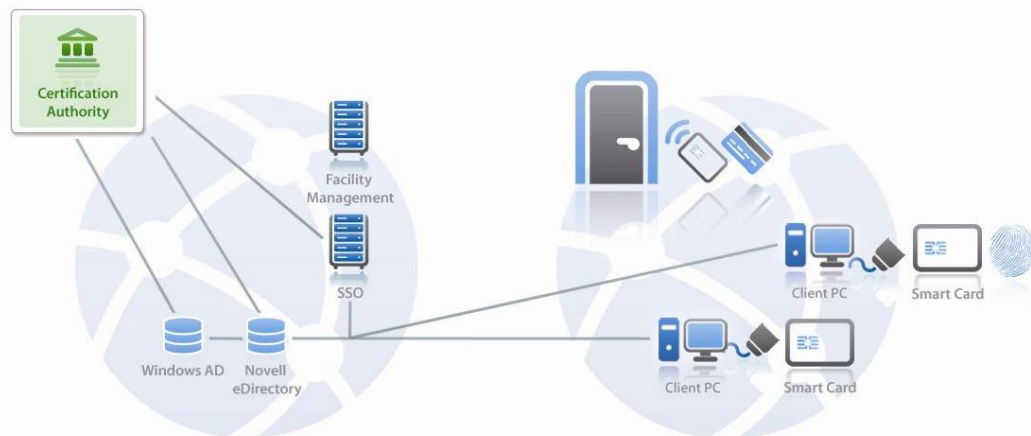
+49-209-167-2477
info@cryptovision.com

*Strong authentication significantly increases security in an internal network. In combination with Single Sign-on it reduces the internal IT costs and the effort for IT helpdesk. This whitepaper describes how strong authentication becomes cost efficient and meets the requirements of SOX and compliance in an enterprise environment. This solution is based on smart cards and certificates provided by the cryptovision products **cv act sc/interface** and **cv act PKIntegrated**.*

During the last years the complexity of company's IT infrastructure increased. Although IT meets many requirements in the internal organization of the industry, companies have to observe the costs of such systems. When it comes to authentication, many enterprises still use passwords. As passwords are not very secure and produce high support costs (users tend to forget passwords, especially, if there are several different they have to remember), it is worthwhile to introduce strong authentication. This is a very efficient way of reducing the costs by reducing the effort for IT helpdesk. Moreover, strong authentication helps to meet several legislative requirements driven by Sarbanes-Oxley Act (SOX) and compliance.

Due to SOX companies have to fulfill several requirements regarding the possibility to trace the usage of IT, addressing questions like: Who has used a system? When was the system used? Which business related actions were authorized? Who else knows about this?). The answers to these questions have to be reliable enough to stand in court. Therefore the basis has to be trustworthy, which is not met by username/password for authentication. Strong authentication is able to raise security and reliability significantly because of the usage of digital certificates and smart cards.

***Strong authentication
– a customer's demand***



Strong authentication with smart cards is a secure way to protect client-server systems and physical access. Especially, smart cards are considered more secure and more convenient than passwords.

Strong authentication as presented in this whitepaper is based on digital certificates and smart cards. A digital certificate can be thought of as a digital passport that is issued to a person. A digital certificate works best if it is stored on a smart card. Smart-card-based digital certificates are considered the most secure authentication technology. If an attacker wants to gain unauthorized access, he needs to steal both the smart card and the PIN of a user (if biometry protection is used, he instead needs to imitate the user's finger print). Therefore, smart cards enable a two-factor authentication.

Strong authentication is especially valuable, when an enterprise uses Single Sign On (SSO). In such a case a user has to authenticate against a SSO client. Afterwards the user is automatically logged into all his remaining applications (like SAP or Lotus Notes). SSO reduces IT costs significantly and has a very positive impact on the IT budget. Moreover, it is a very user-friendly way of handling authentication against several applications, because the user has to login only once. On the other hand, SSO is like a house, which has a locked front door, while every other door to any room opens automatically. In such a scenario, the front door has to be secured in a good way. It is most advisable to use strong authentication to secure the initial login of the user to the computer and to SSO.

Strong authentication in combination with SSO also reduces the costs for internal IT. It helps to harmonize IT processes, because administration of user's passwords for different applications is handled automatically by SSO: No more IT helpdesk calls because of forgotten passwords or locked user accounts. For login the user has to have his smart card available. Beside that the only information the user has to remember is the PIN of his smart card.

In his day to day business a user logs into his PC and the internal network by inserting the smart card into a smart card reader that is connected to the PC. The field for the user name is either filled automatically or no such field occurs (depends on the network infrastructure). A PIN entry field is presented and the user enters his PIN. The user is authenticated after successful certificate validation. If SSO is installed, there is no additional login necessary to any other application; further logins are handled by SSO.

After the user has entered the PIN of the smart card, a digital signature is computed by using confidential data stored on the smart card. The digital signature is transferred to the authentication server together with the certificate. The validation of the authentication on server side consists of three steps: The digital signature is verified by using the user's certificate. The certificate is validated by building the chain to the root certificate that is stored on the

server. The validity of the user's certificate is checked by certificate revocation list (if configured).

If authentication is successful the user is identified based on data included in the certificate. This information is used to decide on the user object the user is authenticated against.

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 card management functions for personalization, initialization, reading/writing data, formatting, PIN change, PIN unblocking and others. While only administrators should have access to the whole set of functionality, there should be a reduced function set (including PIN change) for end users.

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, Unix) and supports all relevant standard interfaces for smart card access – including PKCS#11, Microsoft Crypto-API, Microsoft CNG (Smart Card Minidriver), and ISO 24727. With these interfaces, the middleware can be used with virtually every application supporting smart cards, for instance standard operating systems, office products, single sign-on (SSO) solutions, and web browsers. In addition, **cv act sc/interface** supports two different management components for administrators and end users. While the administrator component complies all management functions, the user component only allows a PIN change and some other simple tasks.

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 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 of 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 identity 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.

The integrated approach of **cv act PKIntegrated** does not require any additional database, because 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

Strong authentication based on certificates and smart cards helps to achieve cost reduction and fulfillment of legislative requirements together with a high level of IT security. **cv act PKIntegrated** is a high-end solution for managing digital certificates. As **cv act PKIntegrated** consequently follows an Identity Management integration approach, it is powerful, lean and cost-effective. If **cv act PKIntegrated** is complemented with **cv act sc/interface** to connect to smart cards it is perfectly suited for securing user authentication against an internal network.

Of course, **cv act PKIntegrated** certificates can be used for much more than only for strong authentication. It as well supports any other security application based on digital certificates: Virtual Private Networks, e-mail encryption, and protecting (W)LAN access can be secured with digital certificates provided by **cv act PKIntegrated**. The more applications a PKI is used for, the more cost-effective it becomes.

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 products refer to: www.cryptovision.com.