



Secure Web Access

A cryptovision whitepaper

Version 1.0

cv cryptovision GmbH
Munscheidstr. 14
45886 Gelsenkirchen

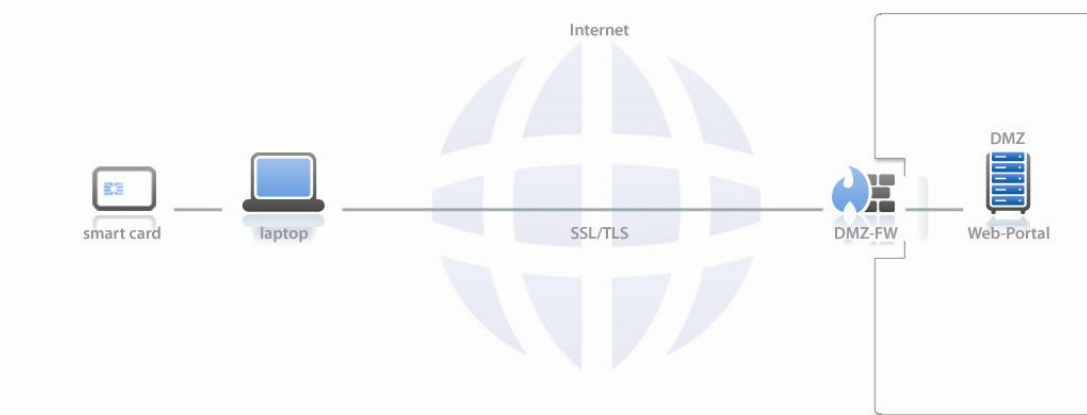
+49-209-167-2477
info@cryptovision.com

When a Web portal is used for business data, security threats are obvious. Therefore, it is necessary to install appropriate encryption and authentication mechanisms. While encryption is quite straight-forward, the decision for an authentication solution is far from being a no-brainer. This whitepaper describes how digital certificates provide a considerable benefit over passwords and other simple Web authentication techniques. Digital certificates can be managed with cryptovision's product portfolio for certificate lifecycle management.

Online-access to corporate data is a business-critical issue in many modern enterprises. Customers need access to their accounts, while teleworkers, field staff, and free-lancers need access to server applications. A Web portal is considered the most flexible solution for these challenges. A Web browser is available virtually everywhere and easy to use. There are powerful solutions for customer portals and online stores. It is also possible to grant employees Web access to their e-mails and to the file system.

However, a Web portal always implies security threats, when it is used for business data. For this reason, the protocol SSL (or TLS) is used to protect Web connections with encryption and authentication. The encryption part is usually straightforward, as all common browsers support strong encryption methods, which are applied without user interaction.

In contrast to this, the choice of an appropriate authentication method in a Web portal is far from being a no-brainer. The most popular methods are passwords. They have the advantage of being cheap and easy to implement. However, the disadvantages of passwords are well-known. Users tend to forget passwords, which results in a high number of helpdesk calls and a loss of productivity. To avoid forgetting a password, many users choose passwords that are easy to guess. Shared passwords and written-down passwords are also common practice. This makes clear that the security of passwords is generally not very high. In addition, IT users have to remember many passwords anyway, so they don't want to be bothered with another one for the Web portal.



Via a Web portal employees, partners, and customers can access corporate data. If smart cards are used, this kind of access is secure.

Advanced Web authentication

As passwords have the mentioned disadvantages, in many cases it is attractive to use a more advanced authentication technology for Web authentication: digital certificates. A digital certificate can be thought of as a digital passport that is issued to a person or to a network component. A digital certificate works best, when it is stored on a smart card owned by the user. Such a smart card solution is very convenient, because the user does not need to remember a password. In addition, smart-card-based digital certificates are considered the most secure authentication technology for VPNs. Their protection is not based on knowledge (like a password), but on ownership – for an attacker it is generally easier to steal something a user knows than an item the user owns. In addition, the user usually notices the theft of an item, which is not the case for a stolen password.

If a smart card without additional access restriction is not secure enough, the card can be protected with a PIN (usually four digits) or with a fingerprint. This means that possession (smart card) is combined with knowledge (PIN) or a biometric trait (fingerprint). Such a two-factor (or even three-factor) authentication provides the highest security level among all practicable authentication methods.

Smart card based Web portal access is especially attractive, when the smart cards are used for other

applications, as well. For instance, an enterprise ID card can be designed as a multi-purpose token suitable for Web portal access, operating system login, physical access and visual application. Such an enterprise ID card considerably enhances both convenience and security.

Of course, instead of a smart card an equivalent microchip device can be used. For instance USB tokens gain more and more popularity, because they don't require a card reader. If not a PC but a smartphone or PDA is used on the client side, smart card chips can be connected via the microSD interface or can be implemented as extended SIM cards. For the respective VPN client it is not relevant, where the digital certificate is stored.

If a corporation doesn't want to use smart cards at all, it is also possible to store a digital certificate in the Web browser. This is less secure and less convenient, because a certificate cannot be easily transferred from one client to another. However, this choice is cheaper and in some cases sufficient.

cryptovision's solution for digital certificates

In order to manage digital certificates, a special component (certification authority) is necessary. A certification authority (CA) is responsible for issuing digital certificates and for an appropriate certificate management. The entirety of components

(especially the CA) and processes used for working with digital certificates is usually called PKI (Public Key Infrastructure).

cryptovision provides the CA 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 an identity management system. When it comes to Web protection, this is a considerable benefit, because automated identity management is already in place in many corporations.

Through its nature as an identity management add-on, it is possible to combine identity management and CA processes. Especially, the registration of new devices or users, the change of device or user attributes, and the deletion of device or user entries can be easily connected with certificate creation, certificate change and certificate revocation. As identity management systems usually contain an extensive set of connectors and drivers, which enable connections to most groupware and human resources solutions, virtually any data source can be used as a basis for certificate lifecycle management with **cv act PKIntegrated**.

In addition, the integrated approach **cv act PKIntegrated** follows has the benefit that 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.

cryptovision's solution for smart cards

When using smart cards for Web portal protection, a smart card middleware implements the connection between the browser 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 like PIN change, PIN unlocking, and card formatting.

The cryptovision product **cv act sc/interface** is one of the most powerful on the market, and it is well-suited for the use with a Web browser. **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.

However, smart card management is more than only managing the content of one single card. In fact it is important for an enterprise to have an overview on all smart cards in use. 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.

Conclusion

A secure Web portal should be protected with digital certificates. **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** and **cv act card/manager**, it is a perfect solution for securing VPN systems.

Of course, **cv act PKIntegrated** certificates can be used for much more than only for protecting Web access. It as well supports any other security application based on digital certificates. For instance, (W)LANs, e-mail encryption, and digital signatures can be realized with the digital certificates provided by **cv act PKIntegrated**. The more applications a PKI is used for, the more economic it gets.

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 **cv act PKIntegrated**, **cv act sc/interface**, and **cv act card/manager** refer to: www.cryptovision.com.