



Workflow Security

A cryptovision whitepaper

Version 1.0

cv cryptovision GmbH
Munscheidstr. 14
45886 Gelsenkirchen

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

Digitally signed workflows make existing processes more secure, and they enable the establishment of new ones. This whitepaper describes how signed workflows work in practice. A focus is put on digital certificates, which are a necessary requirement for digital signatures. cryptovision's product portfolio contains a digital signature solution for workflows as well as products for using certificates and for certificate lifecycle management.

Computer-based workflows have revolutionized business process design in enterprises. The advantages of this technology are obvious: digital information can easily be transported from one location to another – orders of magnitude faster than data printed on paper. In addition, digital workflow information can easily be stored and copied. In fact, digital workflows not only speed up existing processes, but they also enable the establishment of completely new ones.

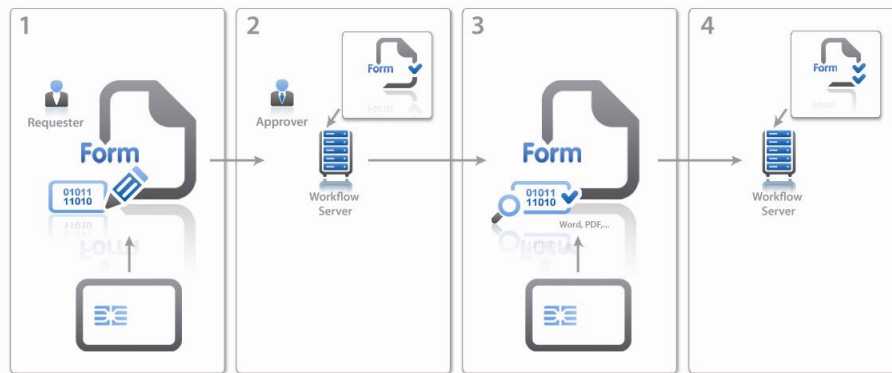
Virtually all branches profit from digital workflows. In a financial services company, for example, a member of the sales staff can enter the data of a new contract. These data are transported over the internet to a server, where they are approved by the sales director. Afterwards, the data are forwarded to the accounting department. There are similar processes in other businesses, like in the capital goods industry or in the retail business.

However, there is also a serious disadvantage of digital workflows: As it is easy to modify digital data,

digital workflows can be manipulated. This is not tolerable in many environments, especially, if high amounts of money are involved in a process. Therefore, many corporate workflows, which could easily be realized digitally, are still carried out in an analog way for security reasons.

Digital signatures for workflows

A well-suited solution for this issue can be set up using digital signatures. A digital signature is not a digitized hand-written signature, but a special kind of check-sum. A secret information ensures that a digital signature cannot be forged, while a public information enables the verification of the signature. Using digital signatures for data has numerous advantages. Digitally signed data cannot be tampered and the signer cannot repudiate that he has signed the data. Therefore, even security-critical processes can be realized in a digital way, when digital signatures are used.



Digital signatures make workflows more reliable. For instance, a person can sign a request (1), which is processed to the workflow server (2), verified by a second person (3) and processed again (4).

For creating and verifying a digital signature, a so-called digital certificate is necessary. A digital certificate can be thought of as a digital passport that is issued to a person (or in some cases to a component). A digital certificate is usually stored on a smart card (or, as an alternative, on an ordinary storage medium), which makes it possible that every user can carry his signature card with him at all times. In order to manage digital certificates, a special component (certification authority) is necessary. A certification authority (CA) is responsible for creating, changing and revoking digital certificates and therefore for controlling the complete certificate lifecycle.

cryptovision's solution

cryptovision provides a solution for workflow signatures called **cv act xml/signer**. **cv act xml/signer** integrates in all major workflow solutions, like the Novell workflow engine, for example. It can easily be used to sign all kinds of workflow data and to verify signatures. Decisions on the further proceeding of a workflow can be based on the result of the signature verification. It is possible to provide workflow data with several signatures from different signers. Of course, **cv act xml/signer** supports smart cards.

When using digital certificates on smart cards, a so-called smart card middleware plays an important

role. A smart card middleware controls 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 like PIN change, PIN unlocking, and card formatting.

The cryptovision product **cv act sc/interface** is one of the most powerful on the market. **cv act sc/interface** runs on several platforms (Windows, Windows Mobile, Mac OS X, Linux) and supports all 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. **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 its assured that sensitive data like a fingerprint is saved on a smart card and not on a PC.

In addition to the components on the client side (signature solution, smart card, smart card middleware), a CA is necessary to support digitally signed workflows. cryptovision provides the CA solution **cv act PKIntegrated** with highly sophisticated certificate management abilities, covering 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 a stand-alone component, but as an add-on to an identity management system. When it comes to digitally signed workflows, this is a considerable benefit, because large corporations usually manage their users with an identity management system. If desired, the CA and the workflow solution can even work with the same user data. Digital signatures based on certificates issued by **cv act PKIntegrated** therefore can be easily assigned to the person (identity) who created it.

In addition, the integrated nature of **cv act PKIntegrated** allows that 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. As identity management systems are specialized on managing identities, it is a beneficial approach to use this functionality for the CA. This way, a CA profits from the fact that identity management systems usually contain an extensive set of connectors and drivers enabling connections to most other user management solutions.

The integrated approach of **cv act PKIntegrated** has the additional 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.

In addition to the digital certificates, the smart cards need to be managed. 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 considerably facilitates the personalization process.

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

Digital signatures are a valuable technology for computer-based workflows. **cv act xml/signer** – combined with other cryptovision solutions – is an ideal tool for this purpose. Workflow data that are digitally signed with **cv act xml/signer** can speed up business processes and enable the establishment of new ones.

Of course, certificates used by **cv act xml/signer** and managed with **cv act PKIntegrated** can be used for other purposes, as well. Among others, Virtual Private Networks, e-mail encryption, and secure Web portals can be realized this way. 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 *xml/signer***, **cv act *sc/interface***, **cv act *PKIntegrated*** and **cv act *card/manager*** refer to: www.cryptovision.com.