



cv act xml/signer – Digital Signatures for Novell® Identity Manager 3.5.x

A cryptovision whitepaper

Version 2.0 (August 2009)

cv cryptovision gmbh
Munscheidstr. 14
45886 Gelsenkirchen

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

The use of digital signatures in corporate IT environments renders a two-fold benefit: it enhances security and saves money. When used to secure workflows, digital signatures are especially valuable, because they can speed up existing business processes tremendously and enable the creation of new business processes. For this reason, the integration of digital signatures into Novell's next generation Identity Manager (IDM 3.5.x) is an important issue. IDM 3.5.x features an improved workflow engine with powerful functions, including a digital signature interface. In this whitepaper we describe how cv act xml/signer works and how it is integrated into an IDM 3.5.x environment. In addition, the benefits of using digital signatures together with IDM 3.5.x are described.

Digital signatures belong to the few technologies that provide a higher security level and lower costs at the same time. The higher security level comes from the fact that digital signatures prevent attackers from tampering with data and provide for non-repudiation. Among the documents that can be digitally signed are orders, contracts, and all kinds of long-term archival data. Current signature algorithms like RSA and ECC are generally considered secure and cannot be hacked even by opponents with a large budget.

Cost-effectiveness is the second advantage that is gained when using digital signatures. Virtually every organization can lower its costs by replacing paper forms with digital forms. Yet, such a replacement is

generally only feasible if there is a digital substitute for hand-written signatures. Digital signatures are designed for this purpose. By changing forms from paper to digital, existing business processes are accelerated, and new ones can be introduced. In addition, digitally signed data are more cost effective to archive in comparison with hand-signed paper documents. In larger organizations there are usually several miles of paper files produced every year — requiring huge storage capacity. In contrast, disc space is cheap and can store millions of digital documents with negligible space requirements.

Digital signatures are especially valuable when used as part of a business work-flow. Current workflows often require that several individuals or roles at

different locations need to sign the same document. Very often, it lasts days before such a process is complete. The reason is that the transport and the processing of the workflow documents is time-consuming, while the action itself usually only requires minimal effort. Many corporations consider migrating workflows from analogue to digital, yet they hesitate because of security or legal issues. The problem is that hand-written signatures are very often a part of a workflow that cannot be immediately changed to digital.

Using digital signatures, it is possible to design workflows that are completely digital, yet render the security and compliance of hand-written signatures. All processed data can be sent over the network. Instead of days, a workflow process may last only a few minutes.

The use of digital signatures in a workflow may be utilized in a variety of ways. They can be used to authorize, approve or submit tasks like granting rights to a specific application, e.g. by a manager for one of his employees or team members. After the manager has digitally signed and therefore approved the task, an automatic action may be carried out – for example, rights to a specific application may be automatically granted to an employee.

Novell Identity Manager 3.5.x

Novell® Identity Manager 3.5.x is a comprehensive identity management suite with support for approval workflows, managing passwords, and managing user data throughout an organization's directories, applications, databases and OS platforms. [novell08]

It is easy to see that digital signatures and Identity Manager's workflow capabilities fit together well. There are virtually infinite numbers of business processes that can be designed using the Identity Manager 3.5.x workflow and requiring the support of digital signatures. Digital signatures can especially be used in Identity Manager 3.5.x, when a user requests a resource (or approves a resource request). This ensures that the user who made the

request (or gave the approval) is really the legitimate person.

The Identity Manager User Application is a Web application which provides the front end for the users. It is used for managing the identity self-service and the workflow based provisioning features. The User Application offers an interface for digital signature support. The digital signature function itself is an optional add-on component. The Admin page of the User Application provides a way to configure and enable digital signature providers. The signature settings for the workflow steps can be defined in iManager or with the Novell Designer for Identity Manager.

xml/signer in detail

xml/signer is the only digital signature solution featuring Novell Identity Manager 3.5.x integration. The integration has been done in a co-operation between Novell and cryptovision.

Though xml/signer is not shipped with the User Application and has to be installed separately [idmdigsig08] the User Application is already pre-configured for the use of xml/signer in the standard installation.

xml/signer is based on cryptovision's cv act library. Thus it supports modern cryptographic algorithms including RSA and ECC digital signatures. Private keys can be stored on a smart card, while other key stores (key file on hard disc, roaming keys with cv act pki/roamer) are also supported.

xml/signer consists of client and server components. The client component's primary functionality is to compute digital signatures for XML data according to RFC 3275. It is a Java applet running in a web browser. The signing procedure is triggered by the User Application via script commands (e.g. JavaScript). Smart cards are supported via PKCS#11 or MS CryptoAPI interfaces depending on the browser type. When the key is not stored on a smart card, but as a software key, xml/signer uses the Mozilla Firefox key store or the Windows key store for Internet Explorer.

In addition, the use of several signing keys is supported (a signing key is a key, where key usage in the digital certificate is set to “digitalSignature” or “nonRepudiation” according to RFC 3280). If more than one signing key is available, the user is prompted to choose one, otherwise the only available key with the appropriate key usage is used automatically.

Before the user submits the form it is possible to preview the data as a raw XML document or as a PDF document. The signed document is sent to the server and optionally a timestamp (according to RFC 3161) can be included (which is required for long-term signatures).

Before the signed document is stored in the database, the User Application invokes the xml/signer server component to verify the signature of the XML document, checks the status of the user certificate and verifies the certificate chain. The server component of xml/signer is integrated into the application server where the User Application is installed. It supports the following features:

- X.509v3 certificates according to the RFC 3280 profile
- X.509 based certificate chain building
- Revocation checking via CRLs
- Revocation checking via OCSP
- RSA, ECC, SHA-1, SHA-2 support
- Seamless integration with cryptovision’s PKI solution cv act PKIntegrated
- Supports virtually any X.509-compliant PKI and smart card solution on the market

Of course, xml/signer needs a CA (certification authority) that provides the certificates that are used for identifying the user [schmeh03]. We recommend cryptovision’s cv act PKIntegrated, which is the only high-end PKI solution on the market with Novell eDirectory integration. cv act PKIntegrated is tailor-made for Novell eDirectory and Novell Identity Manager.

System Requirements

The xml/signer client component is available for both Microsoft Internet Explorer and Mozilla Firefox. Java 1.4, 1.5 or 1.6 is required for using the xml/signer applet.

The server component is installed in the server/lib directory of the same application server instance the Identity Manager User Application has been deployed in (JBoss or Websphere).

Sarbanes-Oxley compliance

One of the major reasons why many organizations currently decide to use digital signatures is the Sarbanes-Oxley Act (SOX). Although SOX is a US law, it not only applies to US companies, but also foreign corporations if they are listed at US stock exchanges.

SOX contains several provisions that can be fulfilled with digital signatures. Most of all, SOX requires that all significant business transactions be initiated, authorized, supported, processed and reported in a secure manner. In particular, systems for detecting fraud have to be installed. All these requirements are solved by digital signatures. If a company listed at a U.S. stock exchange doesn’t comply with these regulations, it may result in severe punishment for the management.

Government Paperwork Elimination Act (GPEA)

Digital signatures have recently gained further importance, due to the Government Paperwork Elimination Act (GPEA). The GPEA is a US law for speeding up administration processes and reducing management overheads by the use of electronic forms and files instead of paper. Digital signatures are explicitly mentioned in the GPEA. Their use is encouraged in order to make electronic processing of security-critical documents possible. In addition, the act states that digital signatures are not to be denied legal effect, validity, or enforceability. It is clear that xml/signer is a valuable product for transforming the GPEA into practical solutions, because xml/signer allows for using digital signatures

in places where paper still plays an important role in workflows.

Conclusion

The use of digital signatures is certainly one of the hottest issues concerning Novell Identity Manager 3.5.x. There are huge numbers of possible applications, all resulting in higher security, faster transactions and lower costs. While the digital signature support of Identity Manager 3.5.x is still a new feature, cryptovision's xml/signer as well as the whole "cv act" family have been on the market for years and are trusted by many customers.

Literature

- [novell08] Identity Manager 3.5.
www.novell.com/documentation/idm35/index.html
- [schmeh03] Klaus Schmeh: Cryptography and Public Key Infrastructure on the Internet - John Wiley & Sons Ltd. 2003
- [idmdigsig08] Evaluation Version of xml/signer
www.cryptovision.com/idmdigsig.html