



## cv act *xml/signer*

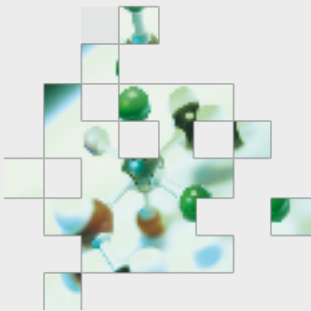
### Digital Signatures for Novell Identity Manager

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 tremendously speed up existing business processes, eliminate paper and enable the creation of completely new business processes. Regarding security, digital signatures provide authenticity and non-repudiation. For this reason, the integration of digital signatures into the Novell Identity Manager is a powerful upgrade. Identity Manager 3.5 features an improved workflow engine with many useful functions including a digital signature interface. For digital signing, the Novell documentation recommends the use of the cv act xml/signer provided by cryptovision, a seamless integrated digital signature solution for Novell IDM.



# cv act *xml/signer*

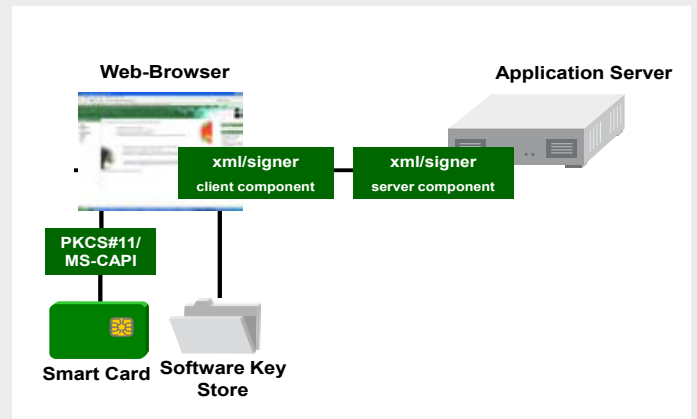
## Digital Signatures for Novell Identity Manager



### Authenticity and Non-Repudiation in Workflows and Approvals

One of the major reasons why many corporations currently decide for the use of digital signatures is the Sarbanes-Oxley Act (SOX). Although SOX is a US law, it doesn't only concern 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 way. Digital signatures have recently gained additional importance because of the Government Paperwork Elimination Act (GPEA). The GPEA is a US law aiming to speed up administration processes and to reduce management overhead by using electronic forms and files instead of paper. Both initiatives are important examples of world wide activities in the field of compliance and regulations demanding the use of digital signatures.

cv act xml/signer consists of a client and a server component. The primary functionality of the client component 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 CAPI 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 while the Windows key store is used for the Internet Explorer.



cv act xml/signer architecture

### Properties

- ▶ Supports Mozilla Firefox and Netscape Security Services (NSS)
- ▶ Supports Internet Explorer and Microsoft Cryptography API (MS CAPI)
- ▶ RFC 3275 compliant XML signatures (XML-DSig)
- ▶ Timestamp interface in accordance with XAdES-T
- ▶ Supports X.509v3 certificates according to the RFC 3280 profile
- ▶ Supports X.509 based certificate chain building
- ▶ Revocation checking via CRLs and OCSP
- ▶ Cryptographic methods RSA, ECC, SHA-1, SHA-2
- ▶ Seamless integration with cryptovision's PKI solution cv act PKIntegrated
- ▶ Supports virtually any X.509 compliant PKI and smart card solution on the market

### System Requirements

- ▶ Microsoft Internet Explorer 6 or higher
- ▶ Mozilla Firefox 2 or higher
- ▶ Java Runtime Environment 1.4 or higher
- ▶ Novell IDM User Application (IDM 3.5 or higher)
- ▶ Novell Audit (Nsure Audit or Sentinel)
- ▶ Timestamp server (optional)

Additional information available at [www.cryptovision.com](http://www.cryptovision.com)

cv cryptovision gmbh  
munscheidstr. 14  
45886 gelsenkirchen / germany

info@cryptovision.com  
www.cryptovision.com  
fon +49 (209) - 167 2450  
fax +49 (209) - 167 2461

cryptovision