

cv act *PKIntegrated*

Integrated Key And Certificate Lifecycle Management

Product Brief



cv act PKIntegrated enhances identity management systems enabling seamless key, certificate, and token lifecycle management. This improves corporate security and enables new business processes which increase productivity.

Management Summary

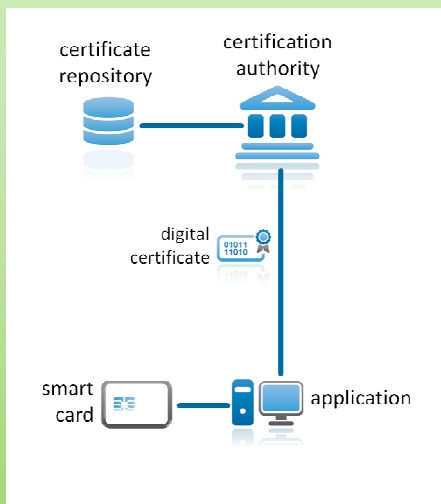
Digital certificates are a fundamental means for e-mail encryption, smart card authentication, and many other security applications. They allow for securely transferring a physical identity into a digital one. Digital certificates are usually issued by a trustworthy certification authority (CA). The whole infrastructure of CA, registration offices, and related components is referred to as Public Key Infrastructure (PKI).

cryptovision's cv act PKIntegrated is a powerful PKI solution. More than 100 enterprises worldwide have integrated cv act PKIntegrated into their identity management systems. The process of provisioning a new identity is combined with the issuance of digital certificates. Other actions in the lifecycle of an identity (e.g. identity termination) are also reflected on digital certificates and incorporated into the online revocation lists.

cv act PKIntegrated is designed as an add-on for an identity management system. It does not require its own database, instead it leverages the existing directory service, allowing for user administration, registration, backup, and workflow functionality with native tools. This integrated architecture not only grants maximum interoperability between identity management and certificate management, but also enables a lean, cost-saving solution improving ROI of the existing identity management system.

As cv act PKIntegrated inherits its administration and registration functionality from the underlying identity management system, cryptovision focus on their core competences of cryptography, PKI, and token integration. cv act PKIntegrated therefore supports a wide range of advanced functions including auto-enrolment, multi-tenancy, card management, certificate management via LDAP, and key roaming.

Background



What Is A Public Key Infrastructure?

For encryption, digital signatures, and strong authentication asymmetric cryptography is a valuable tool. Asymmetric cryptography is based on keypairs, one private and one public. The private key is owned by a certain identity and is not shared. The identity uses the private key to sign, decrypt, or for authentication. The public key, which is shared with the infrastructure is used to encrypt or verify.

In order to bind a key pair to an identity, digital certificates are applied. A digital certificate is a data structure containing the identity's name and public key as the main content. It is signed by a trusted third party (certification authority).

A Public Key Infrastructure (PKI) is the entire combination of components and processes necessary for managing digital certificates. Typical parts of a PKI include the certification authority,

registration authorities, a certificate repository, and PKI applications. An identity in a PKI can either be a person or a hardware device, for instance a PC or a router. A PKI is an important building block of a corporate security strategy, one essential for electronic identity documents. PKI functionality not only enhances the security of eID cards, but also enables additional applications like card-based digital signatures or secure web authentication, enabling new online business processes.

The Basics

cv act PKIntegrated

cv act PKIntegrated is a high-end certification authority (CA) software. In contrast to other CA products, it is realized as an add-on for an identity management system which consolidates identity and certificate management. cv act PKIntegrated is designed to meet high security requirements, complying with all relevant industry standards, including X.509, PKIX, OCSP, and SCEP.

Flexible Registration

All major identity management systems feature flexible registration capabilities – including manual enrolment, bulk registration, user self service, and automated provisioning. As cv act PKIntegrated is integrated into an identity management system, all supported registration scenarios can be applied for PKI enrolment. This makes PKI user registration highly flexible.

Automated Management

cv act PKIntegrated provides fully automated certificate life-cycle management. Certificate generation, certificate renewal, and certificate revocation can be configured to require no administrator or user interaction.

LDAP Interface

cv act PKIntegrated enables the creation, revocation, and renewal of digital certificates via an LDAP interface. Using this feature cv act PKIntegrated can be connected to virtually any external system.

Lean Solution by Integration

cv act PKIntegrated works directly on the user objects of the underlying identity management system and reuses the existing administration interface. It neither needs a separate user database nor an administration interface of its own. This approach makes cv act PKIntegrated lean and cost-effective.

Use of Other IDM Features

Identity management systems usually offer electronic workflow support, sophisticated back-up mechanisms, log data collection, and other useful features. cv act PKIntegrated can be configured to leverage all of them. This makes cv act PKIntegrated highly adaptable without requiring cumbersome infrastructure.

Multi-tenancy

cv act PKIntegrated can be used to operate several CAs with different keys and different policies in one system. Different technical users can access the installation with different permissions.

The Technical Part

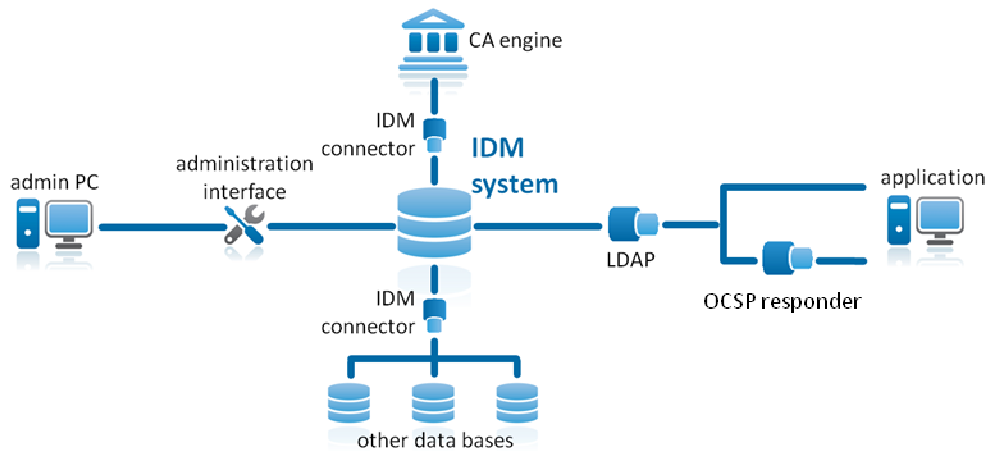
The Architecture

cv act PKIntegrated consists of the following modules:

- **CA engine:** This is the core component, responsible for generating and signing digital certificates (according to RFC 5280 and X.509v3). The CA engine uses one or several keys, which can be stored on a Hardware Security Module (HSM)

Identity Management System

cv act PKIntegrated is designed to be compatible with many different identity management systems, for instance Novell Identity Manager or and IBM Tivoli Identity Manager. The identity management database is used to store user, configuration and transaction data. Via LDAP it can be easily used as certificate repository. If the PKI operator wishes more separation between identity man-



cv act PKIntegrated is integrated into an identity management system. The CA engine, which generates digital certificates, is a stateless component.

for higher security. An HSM is a specialized hardware component, which ensures that the CA keys are not compromised. cv act PKIntegrated supports HSMs via PKCS#11. In addition to RSA it also offers ECC algorithms as specified in the NSA Suite B standard.

- **IDM connector:** A dedicated IDM driver realizes the connection between the CA engine and the IDM system.
- **Administration interface:** cv act PKIntegrated is administered via a plug-in in the administration framework of the underlying identity management system.

- **OCS responder:** This component accepts requests asking for the validity status of a certain digital certificate and replies with a valid or non-valid information. It supports the OCS protocol as described in RFC 2560.

agement and PKI, it is also possible to set up a database exclusively used by cv act PKIntegrated.

Card Management Integration

cv act PKIntegrated can be combined with cryptovision's card management system (CMS) cv act card/manager – a unique CMS following the same philosophy as cv act PKIntegrated. It is even possible to use the management interface of cv act card/manager for operating cv act PKIntegrated.

Auto-enrollment

If an identity is already known in the identity management system, cv act PKIntegrated renders the possibility to automatically create a digital certificate for it (auto-enrolment). cryptovision supplies several add-ons for realizing different auto-enrollment scenarios.

Supported Systems

Identity management system, e.g.:

- Novell Identity Manager
- IBM Tivoli Identity Manager
- Oracle Identity Management
- OpenLDAP

The Market Part

Success story

New York City Transit, the largest public transportation network in North America, is a cv act PKIntegrated customer. The PKI application scenarios at the Brooklyn-based authority include client based e-mail encryption as well as digital signatures for PDF documents, e-mails, and workflow data. Some designated employees work with smart cards managed with cv act card/manager, while others use roaming keys provided by cryptovision's cv act pki/roamer. All PKI users can digitally sign workflow actions with cv act xml/signer as well as perform certificate status checks via an OSCP service achieved with cryptovision's cv act oosp/responder.

New York City Transit, an organization with 12,000 IT users, has been a Novell customer for many years and uses Novell identity management solutions. As cv act PKIntegrated has a seamless integration into the Novell Identity Management suite, certificate lifecycle management was easily integrated into the existing New York City Transit infrastructure.



Customers

cv act PKIntegrated is used (among others) by the following customers:

- **Centrelink:** The Australian social authority Centrelink uses certificates issued by cv act PKIntegrated for a multi purpose employee badge.
- **Husky Energy:** The Canadian energy supplier Husky Energy uses certificates issued by cv act PKIntegrated for securing laptops.
- **Minimax:** The German fire protection supplier Minimax uses certificates issued by cv act PKIntegrated for smart card authentication.

cryptovision

cryptovision is a leading supplier of innovative IT cryptographic security solutions. Based on its 10 year market experience and broad background in modern cryptographic techniques, such as Elliptic Curve Cryptography, all cryptovision products provide the most state-of-the-art and future-proof technologies. The company specializes in lean add-on components which can be integrated into nearly any IT system to gain more security in a both convenient and cost-effective way.

From small devices like citizen eID cards, all the way to large scale IT infrastructures, more than 30 million people worldwide make use of cryptovision products every day in such diverse sectors as defense, automotive, financial, government, retails and industry.



cv cryptovision GmbH · Munscheidstr. 14 · 45886 Gelsenkirchen · Germany
Phone: +49 (209) 167 2450 · Fax: +49 (209) 167 2461

cv cryptovision Inc. · 100 Park Avenue · Suite 1600 · New York, NY 10017 · USA
Phone: +1 212 984 0750 · Fax: +1 212 880 56499