

Product Brief

PKIntegrated

Integrated key and certificate lifecycle management

PKIntegrated enhances the NetIQ Identity Manager, enabling easy and seamless key, digital certificate, and token lifecycle management. PKIntegrated improves corporate security and enables many new business processes which considerably 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, consisting of a CA, registration offices, and related components is referred to as a Public Key Infrastructure (PKI).

cryptovision's PKIntegrated is a powerful PKI solution. More than 100 enterprises world-wide have integrated PKIntegrated into their NetIQ (formerly Novell) 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.

PKIntegrated is designed as an add-on for the NetIQ Identity Manager by Micro Focus. It does not require its own database, instead it leverages the NetIQ eDirectory 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 PKIntegrated inherits its administration and registration functionality from the underlying NetIQ identity management, cryptovision focuses on their core competences of cryptography, PKI, and token integration. PKIntegrated therefore supports a wide range of advanced functions including auto-enrolment, multitenancy, card management, certificate management via LDAP, and key roaming.

What Is A Public Key Infrastructure?

For encryption, digital signatures, and strong authentication asymmetric cryptography is a valuable tool. Asymmetric cryptography is based on key pairs, 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.

Elliptic Curves

PKIntegrated supports Elliptic Curve Cryptography (ECC). ECC algorithms, which are gaining more and more popularity, are more performant than conventional cryptographic methods. Therefore they enable the use of cheaper smart card chips with the same level of security. Several national information security authorities (e.g. the USA-based NSA as a part of the Suite B standard and the German BSI) have committed to Elliptic Curve Cryptography as the preferred technology of its kind. Among others, Microsoft Windows (since Vista) supports ECC.

THE BASICS

PKIntegrated

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

Lean Solution

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

Flexible Registration

The NetIQ identity management system features flexible registration capabilities – including manual enrolment, bulk registration, user self service, and automated provisioning. As PKIntegrated is integrated into the NetIQ identity management system, all supported registration scenarios can be applied for PKI enrolment. This makes PKI user registration highly flexible.

Other IDM Features

The NetIQ identity management system offers electronic workflow support, sophisticated back-up mechanisms, log data collection, role management, separation of duties and other useful features. PKIntegrated can be configured to leverage all of them. This makes PKIntegrated highly adaptable without requiring cumbersome infrastructure.

Automated Management

PKIntegrated provides fully automated certificate lifecycle management. Certificate generation, certificate renewal, and certificate revocation can be configured to require no administrator or user interaction.

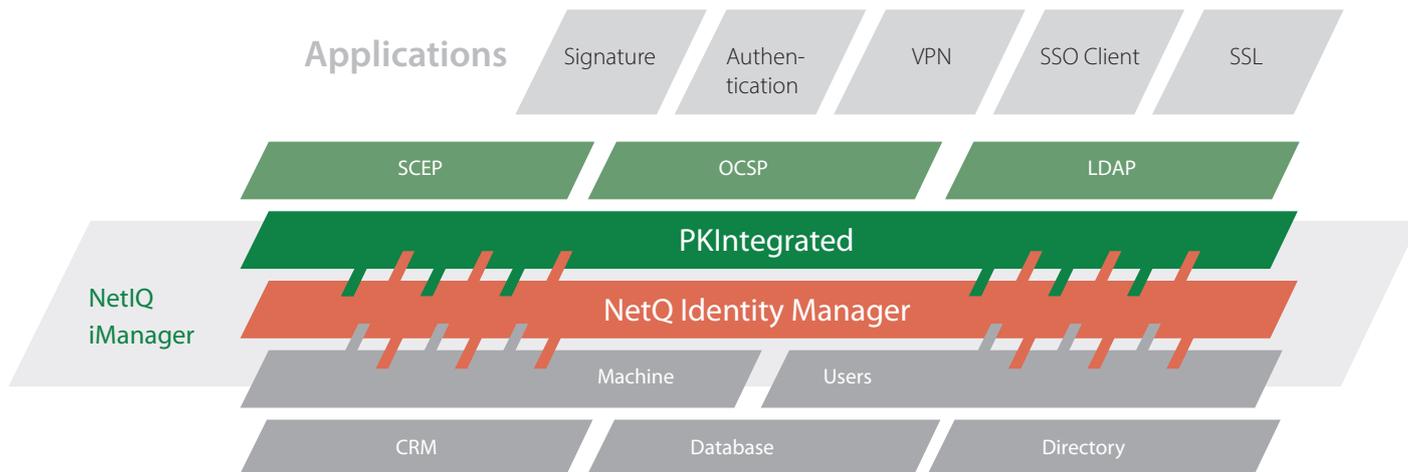
LDAP Interface

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

Multitenancy

PKIntegrated can be used to operate several Certification Authorities with different keys and different policies in one system. Different technical users can access the installation with different accounts.

THE TECHNICAL PART



*PKIntegrated is integrated into the NetIQ Identity Manager by Micro Focus.
The CA engine, which generates digital certificates, is a stateless component.*

The following module types exist:

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) for higher security. An HSM is a specialized hardware component, which ensures that the CA keys are not compromised. 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 NetIQ IDM system.

Administration interface

PKIntegrated is administered via a plug-in in the administration framework of the underlying identity management system.

OCSP 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 OCSP protocol as described in RFC 2560.

Identity Management System

PKIntegrated is designed as an add-on to the NetIQ 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 management and PKI, it is also possible to set up a database exclusively used by PKIntegrated.

Design philosophy

PKIntegrated as well as all other cryptovision products is designed according to a special philosophy. The crypto components are developed by world-leading specialists and integrated into host systems in a minimally invasive way. This approach guarantees that the customer gets the best crypto technology possible without having to waive the IT systems he is used to.

SUPPORTED SYSTEMS

- NetIQ eDirectory
- NetIQ Identity Manager
- Smart card reader or USB port

Success story

The New York City Department of Information Technology & Telecommunications (DoITT) is a cryptovision PKIntegrated customer. DoITT is an agency charged to operate, maintain, and modernize New York City's IT infrastructure. Among other things, it hosts the city's data center. With approximately 1,200 employees operating from five locations, DoITT is one of the largest municipal IT suppliers in the world.

DoITT uses PKIntegrated for service and server certificates. Hundreds of certificates of this kind have been issued to security-critical servers and services across dozens of New York City authorities making the DoITT PKIntegrated installation a critical foundation within New York City's IT security strategy.

The certificate provisioning is integrated into an overarching business workflow system that allows for easy-to-use self-service for some certificates and role based permissions request, review, approval process for other by the authorities' IT administrators.

cryptovision

cv cryptovision GmbH is one of the leading specialists for modern, user-friendly cryptography and secure electronic identities. With its solutions, over 250 million people worldwide and a multitude of institutions in the digital world protect themselves against hacker attacks, manipulation, misuse of identities and espionage.

cryptovision addresses various industries such as public administration, health, automotive, finance & insurance, energy or IT. Its customers include countries such as Nigeria, Ghana and Ecuador, institutions such as the German Armed Forces, the German Federal Office for Information Security (BSI), the city of New York and companies such as E.ON, VW and Allianz. Since 31 August 2021, cryptovision is part of Atos.

CUSTOMERS

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

- Hessischer Rundfunk (HR): The German public broadcasting network uses PKIntegrated certificates for securely connecting IT devices to their corporate LAN.
- Berlin Wasser: The municipal water supplier employs PKIntegrated for secure LAN access, too..
- Universitätsklinik Würzburg: The Bavarian university hospital uses PKIntegrated for securing TLS-servers.



KONTAKT

cv cryptovision GmbH
Munscheidstr. 14
D 45886 Gelsenkirchen

T: +49 209 16724-50
F: +49 209 16724-61
info@cryptovision.com

www.cryptovision.com

