cryptovision

PKIntegrated

Integrated Key And Certificate Lifecycle Management

PKIntegrated enhances the NetIQ Identity Manager enabling easy and seamless key, digital certicate, and token lifecycle management. This 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 of CA, registration offices, and related components is referred to as 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. 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 focus 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.

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 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 by Integration
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 costeffective 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.

Use of 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.

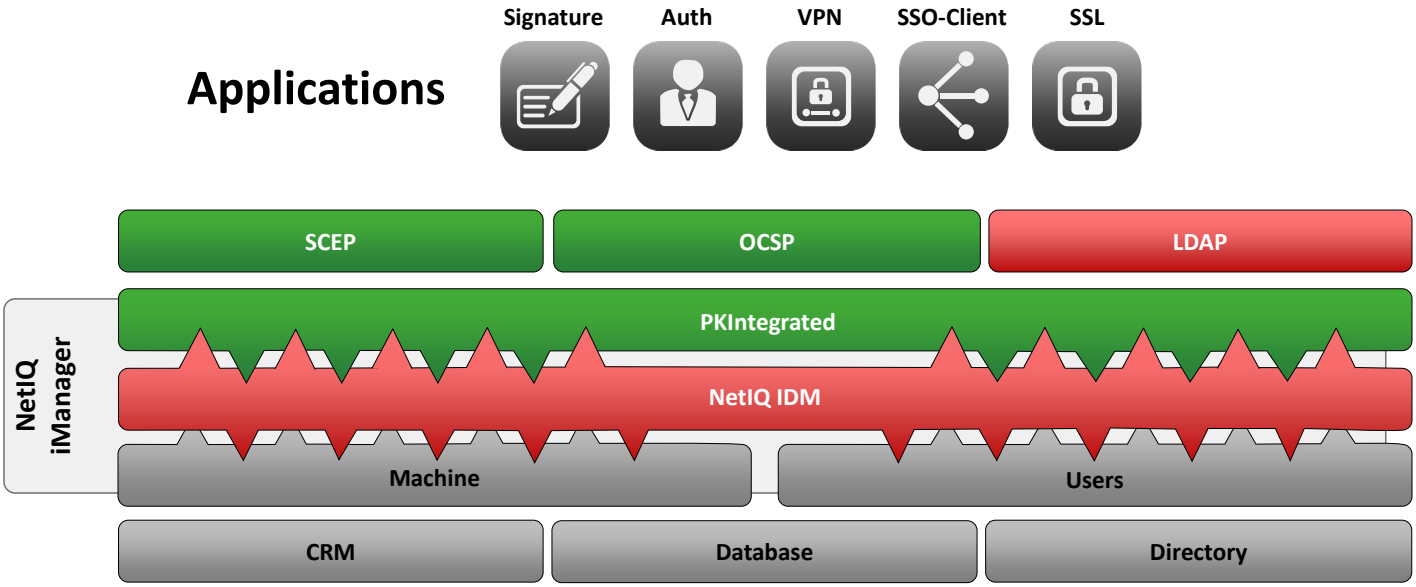
Automated Management
PKIntegrated provides fully automated certificate lifecycle management. Certificate generation, certificate renewal, and certificate revocation can be configured to require no administrator or user interaction.

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

Multi-tenancy
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 accounts.

THE TECHNICAL PART

PKIntegrated is integrated into an identity management system. The CA engine, which generates digital certi - cates, is a stateless component.



THE MODULES

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 off ers ECC algorithms as specifi ed in the NSA Suite B standard.
- **IDM connector**: A dedicated IDM driver realizes the connection between the CA engine and the NetIQ IDM system.
- **Administrations-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 certifi cate 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 developped 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

New York City Transit, the largest public transportation network in North America, is a 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, while others use roaming keys provided by cryptovision's pki/roamer. All PKI users can digitally sign workflow actions with xml/signer as well as perform certificate status checks via an OCSP service achieved with cryptovision's ocsp/responder.

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

Customers

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

- Centrelink: This Australian state authority uses PKIntegrated for managing digital certificates for employee badges.
- Metropolitan Transportation Authority of the State of New York: Largest public transportation agency in North America for IDM.
- Toyota: The world's largest automobile manufacturer uses PKIntegrated for device authentication certificates.

cryptovision

cryptovision is a leading supplier of innovative cryptographic IT security solutions. Based on its 15 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 costeffective way.

From small devices like citizen eID cards, all the way to large scale IT infrastructures, more than 150 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
D-45886 Gelsenkirchen

T: +49 (209) 16724-50
F: +49 (209) 16724-61

cv cryptovision
100 Park Avenue / Suite 1600
New York, NY 10017, USA

T: +1 (212) 984 0750
F: +1 (212) 880 6499

www.cryptovision.com