



Array NetCert Certificate Authority provides full life cycle management of Public Key Infrastructure (PKI) digital certificates that reduces the costs of providing secure, transparent access for employees, vendors, and customers.

Array NetCert Certificate Authority System is a proven solution for issuing, distributing, suspending and revoking digital certificates complete control of user access to applications.

■ **Uncompromising Security**

NetCert Certificate Authority System based on industry standard PKI architecture provides secure X.509 certificates that enable secure interactions between users and multiple applications. Built with all internal communication encrypted and authenticated with digital certificate, internal data and processes cannot be compromised. With audit journals tracking every interaction within the Certificate Authority Server and external components, administrators have complete visibility and corporate compliance requirements are easily met.

■ **Proven Scalability**

Array's NetCert solution has been scaled to meet the demands of some of the largest banks in the world in terms of number of certificates issued and transactions per hour. NetCert supports issuing hundreds of thousands of x.509 certificates per hour and managing millions of active and inactive certificates to ensure secure interactions are completed impact-free. With OCSP real-time certificate checking, NetCert continually maintains an up-to-date secure environment.

■ **Open and Flexible Architecture**

Array NetCert was designed with industry standards in mind to ensure maximum flexibility in meeting corporate needs. Built on strict adherence to Public Key Infrastructure (PKI) architecture along with support for the latest specifications for OSCP, CRL, TLS, and Microsoft Crypto API, NetCert is fully interoperable with 3rd party applications. NetCert's flexibility in choice of popular databases and network directory applications enables enterprise IT operations to fully leverage existing IT infrastructure, training and support. NetCert's flexible multi-certificate system enables users' variable access to applications so productivity is optimized. If their job requirements change, IT personnel can quickly respond by issuing new, canceling or modifying certificates to reflect their changed situation.

Product Highlights

- **Ensures trusted interaction between users and applications via the internet or intranet** with corporate-wide verification policy
- **Proven scalability;** large banking customers with over 5 million certificates on a single server and up to 200,000 certificates issued in an hour
- **Maximum flexibility and interoperability for ease of installation and integration** based on open industry standards such as LDAP v2 and v3, X.509 v3, CRL v2, OSCP, PKCS, SSL /TLS
- **Quick, 'hassle free' client-side certificate installation with NetCert SMART installer** that enables end users to be quickly productive
- **Secure user productivity with multiple applications** as users can have multiple certificates for varied access to different applications
- **Real-time control over application access** with continuous status checking based on OCSP for complete control over access and network security
- **NetCert Infrastructure is completely secured** as communication and data is authenticated and encrypted so identity assets are never compromised

Uncompromising Security

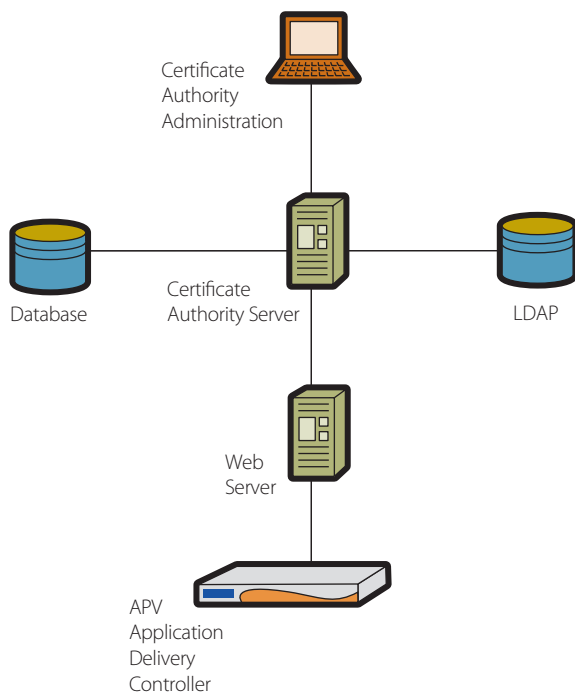
Full X.509 v3 Certificate Services

- Complete lifecycle management of digital certificates for maximum control over access
- Issue and revoke / renew digital certificates
- Suspend and un-suspend digital certificates
- Archiving of expired certificates
- Support for multiple certificate types (Individual, S/MIME, Web, Code Signing, Time Stamp)
- Support for multi-language

Secure Architecture

- Ensures availability and performance of applications with centralized point of management regardless of cluster size
- Digital certificate authentication and SSL/TLS encryption for internal communications
- Communication channels between system components are varied with separate security policies
- Detailed audit journals track access and system errors for meeting corporate compliance requirements
- Divided, role-based administration and certificate authorization for complete transparency
- Server Hardware Security Module Support
- Client hardware token support (G&D, Gemplus)

NertCert Architecture Overview



Flexibility & Scalability

System Flexibility

- Multi-certificate support
- Certificate pattern design for maximum flexibility
- Fault tolerance architecture with support for front-end server load balancing
- Supports a wide range of customization to meet business needs

Full Support For Security Open Standards

- Complete support and with Industry standards specifications and API's for maximum flexibility and interoperability
- X.509 v3
- X.500 DN Standard
- CRL v2
- LDAP v2 and v3
- OCSP
- PKCS #1, 5, 7, 10, 11, 12
- Microsoft Crypto API
- SSL v2, v3 / TLS v1
- Time Stamp

Environment Integration

Corporate Operating System Support

- Support for popular corporate operating systems and networking resources enables simple, intrusion-free implementation and rapid deployment
- Operating Systems Supported
 - Linux (x86 Red Hat Enterprise)
 - Microsoft Windows Server 2003

Corporate Infrastructure Application Support

- Popular corporate infrastructure applications supported for ease of integration and reduced overall management
 - Apache Tomcat
 - BEA Weblogic
 - IBM Websphere
 - Microsoft Active Directory
 - Microsoft IIS Server
 - Novell e-Directory Services
 - Oracle Internet Directory
 - SUN ONE Directory

Popular Corporate Database Support

- IBM DB2
- Oracle
- Sybase