

## *The Robust, Scalable Certification Authority Server*



Public Key Infrastructure (PKI) provides the framework for secure commerce on the net. A Certification Authority (CA) forms the core of this secure framework. The main functions of a CA are issuing Digital Certificates and managing them.

A Digital Certificate contains personal details of the user, his public key and the signature of the CA. It is the electronic equivalent of a notarized document certifying the identity and the credentials of the user, which forms the basis for secure e-commerce transactions.

The Certrix Certification Authority server is an extremely robust, all standards compliant, fully scalable, policy driven certification server with support for commercial strength RSA, DSA and DH Keys. Certificates generated by Certrix comply with X.509v3 standards.

### Key Features

- Comprehensive Certification Authority (CA) system for X.509 certificate issue and management
- Fully scalable, modular, configurable, policy driven and robust CA
- Secure inter-process communication
- Comprehensive library support
- Support for hierarchical CA structures
- Support for multiple RA connections to a single CA
- Multiple interfaces through Web, email and application client
- Support for issue of web browser certificates, server certificates (SSL), e-mail certificates (S/MIME), VPN and code signing certificates
- Support for multiple and user configurable certificate issuance policies
- Database support for Oracle
- Directory system support for LDAP
- Support for OCSP validation
- Key archive service
- Support for Multiple keys and Multiple Certificates per user
- Certificates can be issued in ASN1, PEM, PKCS#7 or PKCS#12 depending on CA policy
- Support for PKCS#11
- Updation of Certificate Revocation Lists (CRLs)
- Comprehensive audit and logging system
- Well-suited for enterprise CAs on the Intranet and Extranet
- Well-suited for Trusted Third Party (TTP) and Commercial Certification Authority (CCA) systems