



CertifyID BlackBox™ - Root Edition

WIS@key unlocks the true power of your internet strategies by enabling cost-effective e-security based on digital identity.

CertifyID BlackBox Root Edition enables any organization or country to establish a full-featured Root Certification Authority (CA) with an extremely low total cost of ownership, by taking advantage of the in-built PKI functionality of Windows Server.

The deployed platform is able to support all typical root requirements and provides the following functionalities:

- Issuance of the Self-Signed Root CA Certificate issued using X.509 certificates (RFC3280)
- Issuance of Signing CA Certificates in X.509 format (RFC3280)
- Use of RSA algorithm for signature generation and verification compliant with RFC3447
- CRL Management
- Secure generation and storage of CA Key Pairs through a dedicated Hardware Security Module (HSM) compliant with FIPS-140 level 2 - 3 standards.
- CC EAL accreditation

This platform provides full flexibility in terms of life-cycle management and can be customized to support duration and validity of the various certificates as well as Certificate Revocation Lists issuance frequency.

Furthermore, in addition to the certification authority functionalities, the WIS@key CertifyID Trusted National Root CA solution, also includes the following additional modules:

- ✓ Secure e-mail
- ✓ Digital signatures
- ✓ Document encryption
- ✓ Secure network communication
- ✓ Secure access control
- ✓ SSL Enabled Secure Servers

CertifyID Platform Components:



WIS@key Guardian for Windows Server CAs

This module adds database redundancy and high availability services to the Windows CA. Installed on top of the Windows Certificate Services, the module runs as a service and stores all Certificates and related information as well as Certificate Status History (the changes of a certificate status during its lifecycle) in an SQL database. Key features are:

- Data persistence - offers permanent high availability storage of certificates.
- CA Disaster Recovery - recovering

the Certificates Services database to its 100% valid state following data corruption or loss.

- Improve the efficiency of certificate management activities by implementing a central certificate information database to support lookup and reporting.
- Implement near-real time data updates - so information remains always up-to-date.
- Implements batch load/update/audit capability - allowing mass loading and update, as well as consistency audits.
- GUI recovery console available separately.

CertifyID Platform Components:



CRL Manager

CRL Manager is a Certificate Revocation List (CRL) mirroring tool that synchronizes the CRL from each CA with its corresponding CDP (Certificate Distribution Point) on the appropriate production Web Server. It also checks hosted CRLs to ensure that they are valid and have not expired. If a valid CRL is not available it immediately notifies the CA operator(s).



CertifyID CA Web Services

The CertifyID MS CA Web Services is a web service API and portal that allows CA administrators and RAs to control, manage and diagnose certificates on the CertifyID Platform. The Web Service closely interacts with Microsoft Certification Authority using strong authentication mechanisms in order to securely query and control Certificates. The CertifyID MS CA Web Services is delivered with an installable client UI that provides remote management of the CA Web Service.

Some of the features include:

- Easy Wizard based Installation
- Easy programmability through Web Service API
- Allows batch certificate requests
- Diagnostic web application portal
- Detailed logging of all interactions
- Uses the HTTP(S) protocol
- SOAP/XML API
- Client neutrality and interoperability:- J2EE, .NET, Python etc.



CertifyID Root CPS/CP Templates & Procedures

WIS@key provides a single-use license for customization and use of a set of Root Certification Practices, Certificate Policies and Procedures for a single Root CA installation. WIS@key professional services can also assist with customization.

Certificate Policy - The Certificate Policy (CP) contains specific information about each type of Digital Certificate issued by the Root CA, as a complementary document of the CPS, and contains the following information:

- Applicability of Digital Certificates
- Registration policies and guidelines
- Allowed usage of certificates
- Digital Certificate subscriber obligations and responsibilities
- Technical structure of Digital Certificates
- Revocation information and procedures

The Certification Practice Statement typically contains the following information:

- Community and applicability of the Root CA structure
- Details and relevant information about the Root CA operator
- Root CA obligations
- Third Parties trusting in the digital certificates issued by the Root CA.
- Liability Limits and Disclaimers
- Financial Responsibility
- Audit Compliance, and Security Audit procedures
- Confidentiality
- Intellectual Property
- Operational Requirements of the Root CA
- Physical, procedural and personnel security controls
- Technical security controls
- Publication and Notification policies
- Law compliance
- Implementation Guide
- Standard Security Requirements and Policies

Key Management Procedure – A template Key Management Procedure (KMP) which specifies the complete Root CA private key lifecycle, and technical and legal procedures related to:

- Root CA Private Key Generation
- Root CA Private Key Revocation
- Root CA Private Key Expiration
- Root CA Private Key Protection
- Root CA Private Key Archival
- Root CA Private Key Backup
- Root CA Private Key Publication

For more information, please visit: www.wisekey.com