



## CertifyID OCSP Server

### Enhanced e-security through real-time validation of digital identities

In today's always online world, managing your digital identity and securing your transactions has become indispensable. Countless institutions worldwide including military, financial, government and corporate are using digital certificates and Public Key Infrastructures to secure physical and electronic access, large financial transactions, and ensure integrity and proof of contracts.

- ✓ Support for multiple CAs
- ✓ Supports multiple validation models
- ✓ Real time validation responses
- ✓ Distributed OCSP architecture
- ✓ Low cost validation infrastructures
- ✓ Robust non-repudiation features

The compromise of a single eID could result in financial losses, forgery, or access to sensitive information. In order to prevent such scenarios, it is imperative that eID status information is communicated quickly and effectively to all users.

The WIS@Key CertifyID Validation Server enables reliable and scalable real-time validation of digital certificates.

#### Ease of use

Based on Microsoft Windows Server 2003, WIS@Key CertifyID Validation Server installs easily and is managed through an integrated Microsoft Management Console.

#### Standards compliance

WIS@Key CertifyID Validation Server handles digital certificate status queries through the use of the IETF RFC-2560 compliant OCSP protocol.

#### Flexible Policy Implementations

Whether out of the box or defined by the registered CA, CertifyID Validation Server supports the implementation of multiple policies. This flexibility enhances the integration of the CertifyID Validation Server within a community of CAs while preserving their independence.

#### Distributed OCSP architecture

Enhanced performance is achieved through the support of a distributed OCSP architecture. CertifyID Validation Server pre-computes OCSP responses for every certificate and delivers these efficiently to front-line relay servers. As these responses are small and do not contain secret data, the relay servers need not be secured allowing for cost-effective deployment.



## CertifyID OCSP Server

Enhanced e-security through real-time validation of digital identities

- ✓ Support for multiple CAs
- ✓ Supports multiple validation models
- ✓ Real time validation responses
- ✓ Distributed OCSP architecture
- ✓ Low cost validation infrastructures
- ✓ Robust non-repudiation features

### Technical Specifications

#### Requirements:

Windows 2000/2003  
10 MB Disk Space  
128MB Memory

#### Standards Support:

FIPS-140-2 L 1,2,3,4 hardware support MS CAPI

#### Supported Hardware

RFC 2560, 3280

### Security Features

The WIS@Key CertifyID Validation Server supports a range of security features, including:

- Robust non-repudiation including digitally signed responses and logs
- Support of FIPS 140-2 Level 2, 3 & 4 compliant cryptographic hardware
- Extensive logging (Event, File, DB)
- Dynamic Real Time Responses
- Distributed OCSP via Pre-Computed Responses
- Direct CA Database Access
  - Real Time Positive Responses
- Security related Email alerts
- OCSP over SSL
- Support of different Trust Validation models
- Multiple Responder Certificates
- Multiple CAs and Validation Policies
- CRL archiving
- Supports
  - CA CRLs
  - Delta CRLs
  - Indirect CRLs
- Proxy and Forwarding



For more information, please visit:  
[www.wisekey.com](http://www.wisekey.com)