



- ✓ Support for multiple CAs
- ✓ Supports multiple validation models
- ✓ Real time validation responses
- ✓ Distributed OCSP architecture
- ✓ Low cost validation infrastructures
- ✓ Robust non-repudiation features
- ✓ CertifyID Guardian XM Certificate Recovery Function
- ✓ CertifyID TrueOCSP Client (Windows Revocation Provider)

CertifyID TrueOCSP (Client/Server)

Real Time Identity Validation with Guardian MX Certificate Recovery Function

Through the combination of two of our cutting edge products (CertifyID Guardian MX and CertifyID OCSP) WIS@Key is able to offer a scalable and unique solution CertifyID TrueOCSP that enables Enterprises to effectively perform **real time** OCSP validations that rely on a common database fed by the Guardian MX tool (Sample Architecture Shown on the back of this Document).

Sample Customer Application:

Organisations using a Windows Smart Card log-on desktop mechanism, now have the added functionality and security to perform seamless and immediate validation of identities during the authentication process.

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.

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 TrueOCSP Suite (Client/Server)

Windows Smart Card Scenario



Microsoft Certificate Services and CertifyID Guardian XM Exit Module



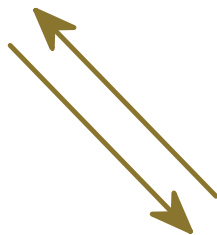
CertifyID SQL Server Database



Active Directory with the CertifyID OCSP Client



CertifyID True OCSP Server



Windows Smart Card Log-On

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