

KeyOne Desktop

Document Protection



KeyOne Desktop

KeyOne Desktop is an advanced desktop tool that enables the protection of any document through digital signature and data encryption.

- It is completely integrated with Windows' file explorer.
- To be used in applications, providing data protection functionalities.
- Provides management tools for configuration of signature policies in a centralised manner and guarantees the maintenance of protected data access privileges during time.

Functions

KeyOne Desktop offers a client data protection environment based on Public Key Infrastructure (PKI) that can be managed by the user or centrally by an authorized administrator. The provided functionality can be accessed as a service ready to be used by corporate applications or by the user's interface.

- **Electronic signature and encrypted data.** KeyOne Desktop has been designed to sign with or without time stamping feature and to encrypt data from Windows file explorer. It maintains its own recognized Certification Authority management and facilitates the verification of the certificate status while consulting the revocation list or the Validation Authority.
- **Integration component.** KeyOne Desktop's security environment can be used as a security service through SOAP (Simple Object Access Protocol) transactions, via XML language providing simple access to corporate applications of the configured security mechanisms that are easy to program.
- **Centralized configuration.** The definition and maintenance of signature policies as well as the protection of data can be carried out in a totally centralised manner, offering unique security and management guarantees that add convenience value to users.
- **Control access to encrypted data.** All access privileges for encrypted data can be managed by the user adjusting it to the corporate's privilege management. By doing so it guarantees the maintenance and access in the long run (even when the ciphering certificate has expired).

Benefits

- **Smooth configuration, maximum security and control.** Within corporate environments, the functionalities of the system and data access privileges are defined in a centralized manner, providing a smooth management as well as preventing workstations from any manipulation. The unique management of Desktop's security environment allows the administrator to define security parameters, signature policies and access privileges for encrypted data in a transparent way for the user; and it guarantees a secure system that is easy to use.
- **Interoperable and standard.** Thanks to Safelayer's commitment towards security standards, KeyOne Desktop's security environment is interoperable with most important certification service providers. It also guarantees the possibility of securely exchanging documents and electronic mail with other companies or clients.
- **Rapid and smooth integration.** Due to the development of web services standards, the introduction of security in applications implies the consumption of specialized services. KeyOne Desktop's security environment incorporates an open and advanced interface programming that simplifies the integration and maintenance of security mechanisms in applications, maximizing cost savings and leveraging your return on investment.

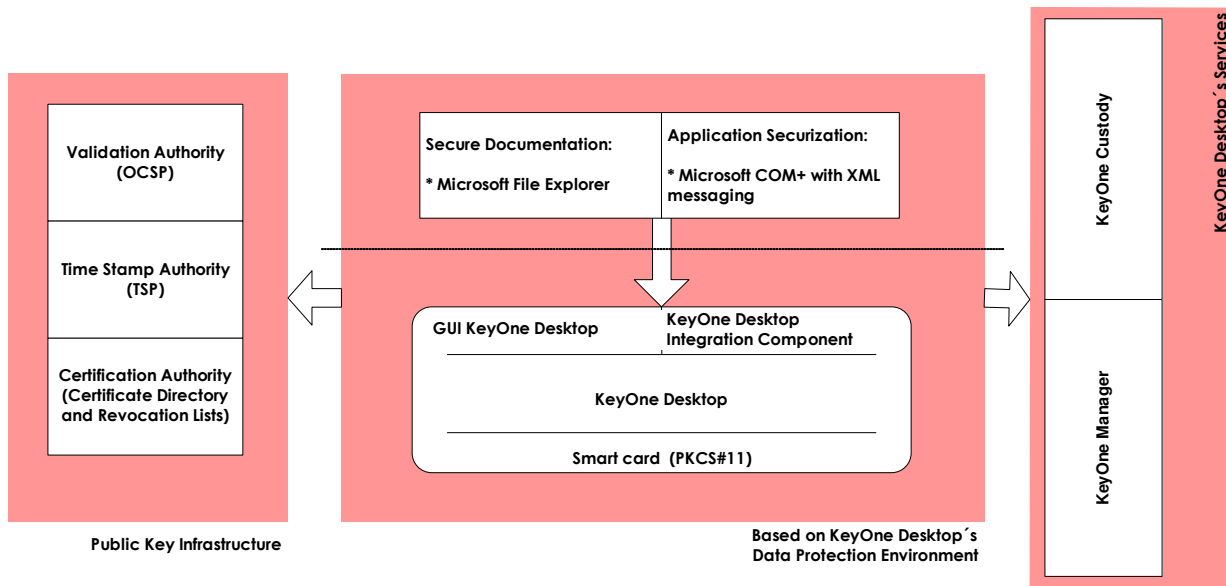


KeyOne Desktop



Architecture

KeyOne Desktop application integrates with Microsoft Windows Explorer. KeyOne Desktop's Integration Component and KeyOne Desktop's Services are optional components. The platform also allows for the inclusion of Safelayer's KeyOne solutions (KeyOne CA, KeyOne RA, KeyOne TSA and KeyOne VA) and/or it can operate with external public key infrastructures:



- **KeyOne Desktop:** An application that provides a basic security environment, consisting of KeyOne Desktop and a smart card through a PKCS#11 interface certified by Safelayer.
- **KeyOne Desktop's Integration Component:** Provides the interface to access corporate applications in a secure manner enabling the application to use the security mechanisms offered by KeyOne Desktop.
- **KeyOne Manager:** Optional service that manages signature and data protection policies in a centralized manner.
- **KeyOne Custody:** Optional server to manage privileged access of protected data in a centralized manner through encryption.

Technical Characteristics

- **Standards for electronic envelope:** IETF CMS/PKCS#7, IETF S/MIME. Consult for IETF's digital signature for PDF in PKCS#7.
- **Electronic time stamp:** IETF TSP Time Stamp Protocol.
- **Digital certificate formats:** ITU-T X509v3.
- **Verification of digital certificate status:** Using CRLs or IETF's OCSP protocol.
- **Directory support:** LDAP protocol and Microsoft Active Directory to download certificates.
- **Smart card support:** PKCS #11 devices certified by Safelayer.
- **XML interface support for Microsoft COM+:** Based on OASIS's DSS (Digital Signature Service) standard that uses SOAP transactions in XML language together with COM+ as transport mechanism.

System Requirements

- **KeyOne Desktop:** Microsoft Windows 2000 and XP.
- **KeyOne Manager:** Microsoft Windows XP Professional SP2 (32 bits) or Microsoft Windows Server 2003 Enterprise Edition SP1. Microsoft IIS 3 or superior. Microsoft Internet Explorer 4 (SP1) or superior. LDAP Server Netscape Directory 4.2 or superior.
- **KeyOne Custody:** Information on request.

SAFELAYER SECURE COMMUNICATIONS S.A.

c/Basauri, 17 Edif. Valreality Edif. B Pl. Baja Izquierda Ofi. B 28023 Madrid (SPAIN) Tel.: +34 91 7080480 Fax: 91 3076652
Edifi. World Trade Center (S-4) Moll de Barcelona s/n 08039 Barcelona (SPAIN) Tel.: +34 93 5088090 Fax: 93 5088091

WWW.SAFELAYER.COM