CompEd®
Software Design

Software Solutions for the
Digital Document World

Technical Description

DigitalSign® 3.1

State of the art legally valid electronic signature

The best, most secure and complete software for

- **Adding digital signatures to any document, in conformance with European laws**
- **Opening and utilizing signed documents, verifying the validity of signatures with maximum reliability**
- **Attaching timestamps thus ensuring the validity of digital documents**
- **Encryption and decryption of document contents protecting them from unauthorized readers**
- **Using smartcards provided by the most important Certification Service Providers**

DigitalSign can be integrated into any application aimed at manipulating digital documents and/or electronic signatures

DigitalSign 3.1 is state-of-the-art electronic signature software.

An evolution of *DigitalSign 3.0* – the reference digital signature software – combines in a single product absolute completeness, great ease of use, exemplary presentation efficiency and extreme flexibility, with strict compliance to EU laws, standards and security principles.

1. Description of main functions

1.1 Generation of electronic features

DigitalSign 3.1 generates documents into a standard CAdES (evolution of PKCS#7) format from any type of digital document.
The user can open an existing document or create a new one (*ActiveDocument*, see 1.6) by a simple click, automatically viewing the document content through the dedicated window; the digest of the document – on which the signature will be calculated – is immediately shown

With a second click on the "Sign" button the user can then add his own electronic signature, and immediately view the verification results of the signature itself.

With a last click the user can save the results onto a PKCS#7 file.

The user can even open a document signed by someone else, in order to add his/her own electronic signature (as a parallel signature or a counter-signature) and save the result using the same easy procedure.

If desired, DigitalSign can even handle multiple PKCS#7 envelopes; a signed document containing another signed document and so on.

With each signature a "signing time" attribute can be associated - useful for indicating a time reference and required by some tax regulations.

1.2 Timestamp attachment

In order to ensure the strength of a digitally signed document as evidence, it is strongly recommended associating the document itself with a timestamp.
Thanks to a timestamp it then becomes possible to fix the time in which the document was signed and thus "officialized" to the time referred to by the timestamp.
As a consequence, the later availability of such a piece of evidence enables the user to claim that the signature was valid when accepted (by comparing the timestamp with the actual date of expiry or revocation of the signer's certificate).
A timestamp thus extends the 'legal validity' of a signed document beyond the validity time of the certificate used to sign it.
Timestamps with DigitalSign can be handled:

- as separate entities with respect to the associated document (association simply relies on file names);
- as compound entities, by means of enclosure of both the document and the timestamp in a single RFC 5544 structure;
- integrated in the CAdES-T document: each single signature can be provided with a specific timestamp as a signature attribute

Regardless of the selected association method, ***DigitalSign 3.1*** always shows a timestamped document in a single window, immediately reporting verification results (of signatures and timestamps) and if desired, demonstrating that the document is considered valid thanks to the presence of a timestamp.

The user can configure several timestamping accounts, related to different providers (TSA), and use the preferred account at any time.

DigitalSign 3.1 supports ETSI TS 101 861 V.1.2.1 and RFC 3161 specifications for timestamping.

1.3 Encryption/decryption of document contents

DigitalSign 3.1 supports content encryption inside PKCS#7 envelope, by means of a standard combination of symmetric + asymmetric cryptography.
This technique allows the user to produce documents that are only signed, only encrypted or both signed and encrypted.

When the user decides to make a document visible to a group of recipients only, DigitalSign automatically generates an encryption key – called 'session key' – using the highly secure 3-DES symmetric algorithm; such key is then used to encrypt the document.
The session key itself is then encrypted using the public key of all selected recipients (taken from their certificates) and such encrypted versions are stored together with the encoded document.

Later, the owner of a private key that matches one of the public keys used at encryption time will be able to use his/her own private key to decrypt the session key and then to use such session key to decode, display, print, export the original document.

In accordance with regulations about advanced electronic signature and with security principles, signature keys and certificates are not used for any different purpose; therefore different keys and certificates are used for encryption, but they must be contained in a signature device (smartcard) in order to be usable by DigitalSign.

Following options apply:

- the user can directly use certificates (and related keys) provider by CAs as auxiliary items (defined as 'authentication', 'SSL', 'for email', etc.) on the same smartcards containing signatures certificates;
- the user can also generate his/her own keys (or an organization can take care of this task) for encryption by means of the Personal Certification Authority (see section 1.8)

1.4 Verification of electronic signatures

DigitalSign 3.1 is a superb instrument for verification of electronic signatures, capable of unparalleled performance in terms of reliability.

When a digitally signed document is opened all signatures are instantly verified and results are displayed in an information panel shown below the document window.

The information panel shows separately the verification results of document integrity and the verification results of the signers' certificates (thus signers' identities).

Depending on the configuration set by the user (i.e. unless the user disables some options), DigitalSign performs verification of a certificate as follows:

- validity state (not expired);
- status of qualified certificate (i.e. issued by an accredited CA);
- if previous step is not fulfilled, status of trusted certificate (CA included in a specific list, protected itself by means of a qualified electronic signature);
- state of suspended or revoked (by checking the appropriate CRL – Certificate Revocation List – published by the issuing CA);
- extension of validity by means of an associated timestamp, if applicable.

NOTE: the present implementation of DigitalSign is tailored to take advantage of the high degree of security offered by Italian law: publication of an official – and signed – list of accredited CAs.
CompEd is available to consider implementation of different modules for authentication of accredited CA lists.

If the user decides to reduce the level of security of his/her own workstation (e.g. by de-activating CRL verification against CRLs because an Internet connection is not available) the information of the reduced level of security is always displayed together with verification results.

From December 2009 Italian Certification Provider are required to keep the revocation/suspension information in the CRLs even after certificate expiry.
As a consequence, by checking the current CRL, the verification software knows whether a certificate – even an expired one – was valid or not at a given date and time in the past.
DigitalSign allows the user to enter a past date and verify the validity of a document at that time.
Of course if a document – or a single signature – is timestamped, the verification is automatically referred to the timestamp date and time.

The secure verification of an electronic signature is an extremely delicate process requiring the availability of a secure point of reference or *Trust anchor* to rely upon.

DigitalSign 3.1 adopts the following measures:

- Trust anchor directly consists of an official list of accredited CAs, published and kept up to date by a Scheme operator (DigitPA in Italy) at an official Internet address and protected by an official electronic signature (related thumbprint officially published);
- Automatic update of the local copy of the official list, according to a time schedule defined by the user;
- verification of the electronic signature(s) protecting the official and/or user-defined list(s) at every application start and subsequent dynamic creation of a memory-based trust list
- Internet address of official CA list and thumbprint of the certificate used to sign the official list hardcoded in DigitalSign itself;
- Self-integrity check system (based upon a digitally signed hash table) to ensure that the executable code of DigitalSign has not been tampered with.

At document opening time DigitalSign also shows warning messages in case the document contains – or may contain – variable elements or macro-code that may cause the loss of legal validity of the signed document.

1.5 Signature devices, supported smartcards, automatic recognition

A certification service provider that distributes qualified certificate to be used in conjunction with SSCE – Secure Signature Creation Devices – has the responsibility (often regulated by law) to deliver the device itself or to manage its initialization, in terms of key-pair generation and certificate installation.

The most widely used standard for such devices is PKCS#11: the electronic signature software needs to interface with a device (commonly a smartcard or an USB token) through a specific software module (a sort of driver) provided with the device.

Even within the PKCS#11 specifications some differences exist in the behavior of different devices and/or PKCS#11 modules; in addition some Certificate Service Providers organize data in different ways on a devices' memory.

One of the primary targets of ***DigitalSign 3.1*** is to allow the user to make use of smartcards issued by any Certification Service Provider. At present all smartcards and USB tokens distributed by Italian accredited CAs are supported by ***DigitalSign 3.1***. CompEd is available to test any new devices and – if required – to implement specific interface modules/workarounds with the aim of expanding the list of supported devices.

By means of a very effective feature of automatic recognition of the mounted device, ***DigitalSign 3.1*** also makes the interface procedure extremely easy.
When the user inserts a different smartcard into the reader, DigitalSign automatically tries to access the card through all PKCS#11 modules installed on the computer and in a few seconds, the connection is made.
Of course the procedure begins with the last successfully used module in order to make the connection as quickly as possible when using the same device each time.

At present the automatic recognition module has been tested with a wide number of PKCS#11 modules, distributed with signature devices used in conjunction with qualified certificates.
The user can also make a manual configuration as well as install other PKCS#11 modules, which can be added to the list of modules to try for automatic recognition.

Some new digital signature systems, based upon centralized servers used remotely – instead of personal devices, are encountering market success nowadays.
When these systems offer PKCS#11 interfaces DigitalSign can immediately use them.
For other cases, when these system provide proprietary interfaces, CompEd offers a technology named "Virtual P11": a software module can be customized to such interface – server side – and connect to DigitalSign through PKCS#11 standard.

1.6 SecurView: presentation of documents integrated with most popular software

When the user adds an electronic signature to a document it seems reasonable that he/she wants to view the document contents carefully.

But when using a PC it is sometimes not so obvious that two different applications (for example the wordprocessor or the web browser and the electronic signature software) are actually working on the same data.

The potential risk lies in the possibility that – maybe due to an error – the user sees one document and signs another.

DigitalSign 3.1 offers an integrated environment, where the document contents are displayed within the same window that also contains the commands to sign, encrypt and timestamp the document; and where the results of verification of signatures and certificates are instantly shown.

Because users want to use their favorite productivity tools and because resulting documents are produced in several formats, DigitalSign has had to address the problem of a coherent – and integrated – handling of different types of documents.

DigitalSign's SecurView is the solution. This document viewer handles:

- the opening of documents compliant with ActiveDocument standard (basically those edited with Microsoft Office products and with CorelDraw); allowing editing in the DigitalSign window through the original application;
- the opening of HTML and XML documents using the OCX of MS Internet Explorer;
- the opening of PDF documents using Adobe Acrobat or Adobe Reader
- the opening of text or RTF documents using a specific built-in viewer
- the opening of image documents (TIF, JPG, GIF, BMP, …) through a specific built-in viewer, based on Lead graphics technology.

1.7 Reports on the details of a signed document

Sometimes a document contains a large number of significant items (multiple signatures and/or countersignatures, encryption recipients, certificates, timestamps, copies of CRLs, …) and it is desirable to have a complete, printable, exportable presentation of such attributes and details.
DigitalSign 3.1 contains a new feature to produce such a report in HTML format, easy to export, save, print and merge with other documents.

1.8 Generation of in-house certificates (Personal Certification Authority)

Some application contexts exist where it is not necessary to use qualified certificates issued by accredited CAs, but an organization can choose to utilize certificates produced in-house, based upon standards and associated to key-pairs securely generated inside cryptographic smartcards. Moreover, even if European laws require the usage of qualified certificates in order o achieve maximum legal validity of electronic signatures, no legal restriction applies to certificates used for encryption.

The user can use the Personal Certification Authority of DigitalSign to:

- initialize and setup blank smartcards or soft tokens
- generate certification key-pairs and CA certificates, then usable to issue end-user certificates;
- process certificate requests coming from end-users thereby generating related certificates;
- create and manage revocation lists (CRL) in order to terminate the validity of certificates of users who lose their smartcards or certain qualifications inside the organization.

Certificates produced with this tool, thanks to new security features of ***DigitalSign 3.1*** (see section 1.4) can be trusted and verified at the same security level (strong) applied to certificates issued by accredited CAs.

Normally a single Personal Certification Authority is enough to fulfill the needs of certificates of a small-medium size company or organization.

As an example, DigitPA (the Italian Governmental department in charge to supervise the Certification Service Providers' activities) makes use of the Personal Certification Authority of DigitalSign 3.1 to manage the special CA used to sign the official list of Accredited CAs.

1.9 Activity log

DigitalSign 3.1 contains an activity log module to keep an accurate record of all significant activities performed by the application, including the date and time of each event.

1.10 User interface

DigitalSign 3.1 offers a very sophisticated user interface, while being easy and intuitive at the same time.
The user can keep several documents open at the same time (MDI), view some general information panels about current hardware and software configuration, customize toolbars and access configuration panels.

No other electronic signature product equals DigitalSign in terms of display effectiveness; rendering at a glance document contents and other important items such as signatures, timestamps, certificates, hash codes, etc.

1.11 Programming interfaces: Developer License

DigitalSign 3.1 is the ideal tool for a developer or a system integrator who needs to introduce the management of digitally signed documents into document management or workflow applications, as well as in "vertical" products in the fields of hospital and medical organizations workflow, public administration, private enterprises.

Many software houses have already chosen DigitalSign for very solid reasons:

- undoubted technological superiority and proven reliability
- actual and verifiable independence from the specific services of different CAs: the investment in terms of development is safe, regardless of

the choice of the end-user about the Certification Provider;
- high integration quality thanks to the DigitalSign ActiveX – making the powerful GUI of DigitalSign available to the programmer – and the extremely rich and powerful COM interface
- richness of functions that allow the user to realize digital signature procedures based upon the ActiveX using a surprisingly low number of instructions, or 'silent' procedures supported by user interfaces redesigned by the programmer; moreover the programmer can develop automated routines to generate batches of signature in unattended way.

Three interfaces are available:

- an ActiveX component that makes it simple to integrate a typical document window of DigitalSign into any application, even web-based, showing/hiding/driving the original toolbars;
- an extremely rich COM interface organized into categories, exposing methods and properties at different abstraction levels;
- an interface for the development of add-ins, useful for enriching and customizing the behavior of DigitalSign.

The usage of DigitalSign API is reserved to the subscribers of a Developer License.
Different licenses are available for end-users whose aim is to integrate DigitalSign in applications for their own usage and for those companies or professionals whose aim is to distribute integration results.
More information can be obtained by writing to info@comped.it

2. Operating environment and system requirements

DigitalSign 3.1 supports Windows operating systems, from 2000 SP1 to Windows 7.
Internet Explorer 5.0 or greater is also required.

In case of usage of smartcards or other devices at PKCS#11 level, the specific PKCS#11 software module is distributed by the provider/supplier of the token itself and may show compatibility requirements more restricted than DigitalSign.
Moreover, in such a scenario, the PKCS#11 software controls the card reader or other hardware, consequently the choice of a smartcard reader should be made in accordance with the specifications of the smartcard supplier.

3. Available editions

DigitalSign 3.1 is available in the following editions:

- **Professional –** the complete edition, containing all features described in this document.
- **DigitalSign Reader –** an edition not containing "active" features, but allowing opening, displaying ad the verifying of electronically signed and timestamped documents.
  It can be downloaded from CompEd web site and used by non-professional users for private usage, or by subjects who just "use" documents signed with CompEd software.