
Technical Description

DigitalSign[®] 3.0

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 confidentiality
- 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 3.0 is state-of-the-art electronic signature software.

An evolution of DigitalSign 2.0, *DigitalSign 3.0* 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 principles of security.

1. Main functions

1.1 Generation of electronic features

DigitalSign 3.0 generates documents into a standard PKCS#7 format from any type of digital document. The user can open an existing document or create a new one (*Active Document*, 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 results 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 time stamp. Thanks to a time stamp, it then becomes possible to establish the time in which the document was signed and thus “officialized” to the time referred to by the time stamp.

Consequently, the later availability of such evidence enables the user to claim that the signature was valid when accepted (by comparing the time stamp with the actual date of expiry or revocation of the signer’s certificate).

A time stamp thus extends the ‘legal validity’ of a signed document beyond the validity time of the certificate used to sign it.

Time stamps with DigitalSign can be handled:

- as separate entities with respect to the associated document (association simply relies on file names);
- or as compound entities, by means of enclosure of both the document and the time stamp in a single MIME structure.

Regardless of the method of selected association, *DigitalSign 3.0* always demonstrates a time stamped document in a single window, immediately reporting verification

results (of signatures and timestamps) and if so desired, demonstrating that the document is considered valid due to the presence of a time stamp.

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

DigitalSign 3.0 supports RFC 3161 for time stamping. In addition, specific support modules for proprietary servlets adopted by popular time stamping providers are available.

1.3 Encryption/decryption of document contents

DigitalSign 3.0 supports content encryption inside a 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; this 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 these 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 that session key to decode, display, print, and/or 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 other purpose; therefore, different keys and certificates are used for encryption, but they must be contained in a signature device (smartcard) in order to be utilized by DigitalSign.

The 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 3.0 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 separately shows 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:

- state of validity (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 time stamp, 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.

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 3.0 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 (CNIPA 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;
- automatic update of the local copy of the official list, according to a time schedule defined by the user;

- Internet address of official CA list and thumbprint of the certificate used to sign the official list hard coded 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 displays 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.

he most widely used standard for such devices is PKCS#11: 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 behaviour 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 3.0** is to allow the user to make use of smartcards issued by any Certification Service Provider. At present DigitalSign 3.0 supports all smartcards and USB tokens distributed by Italian accredited CAs. 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 3.0** 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 within 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 PKCS#11 modules by Cryptovision, Gemplus, IPM, Siemens.

The user can also produce a manual configuration as well as install other PKCS#11 modules, which can be added to the list of modules to test for automatic recognition.

But PKCS#11 is not the only way to interface a signature device, in case the user wants to produce certificates on his/her own at an organizational level, rather than adopt devices and certificates issued by accredited CAs, DigitalSign can interface some smartcards and USB tokens at APDU level (i.e. at low-level, based upon detailed specifications of devices). This implies better performance, greater flexibility and integrated services to set PIN/PUK passwords, for storage of user data in the device memory, etc.

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 word processor 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 3.0 offers an integrated environment, where the document contents are displayed within the same window, which also contains the commands to sign, encrypt and time stamp the document; and where the results of verification of signatures and certificates are instantly shown.

Because users want to use their favourite 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
- 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, time stamps, copies of CRLs,) and it is desirable to have a complete, printable, exportable presentation of such attributes and details.

DigitalSign 3.0 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, an organization can choose to utilize certificates produced in-house, based upon standards and associated to keypairs securely generated inside cryptographic smartcards. Moreover, even if European laws require the usage of qualified certificates in order to 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
- 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 3.0** (see section 1.4) can be entrusted 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.

1.9 Activity log

DigitalSign 3.0 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 3.0 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 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, time stamps, certificates, hash codes, etc.

1.11 Programming interfaces: Developer License

DigitalSign 3.0 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 into "vertical" products in the fields of hospital and/or medical organizations workflow, public administration, and 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 *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 and using a surprisingly low number of instructions, or 'silent' procedures supported by user interfaces redesigned by the programmer. Moreover, the programmer can develop routines to automatically generate batches of signature.

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 behaviour 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 into applications for their own usage and for those companies or professionals whose aim is to distribute integration results.

Ulterior information can be obtained by writing to info@comped.it.

2. Operating environment and system requirements

DigitalSign 3.0 supports Windows 98, Me, NT 4.0 (Service Pack 4 or greater), 2000 (Service Pack 1 or greater), XP operating systems.

Internet Explorer 5.0 or greater is also required. For reasons of security and/or reliability, it is recommended to use DigitalSign with Windows NT, 2000 or XP.

In order to use automatic CA list update features, verification against CRL and time stamping services, an Internet connection that supports http, https, and ldap protocols is required. Compatibility with company proxy servers that require user authentication should be verified in advance.

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 3.0 is available in the following editions:

- **Professional** – the complete edition, containing all features described in this document.
- **Lite** – a reduced edition, downloadable from the CompEd web site, free license available for non-professional usage by private users.

It does not support encryption/decryption of documents, cannot attach timestamps, cannot add multiple signatures/countersignatures to documents, does not contain the Personal Certification Authority and the Activity Log

subsystem. Nor does it support programming interfaces.

- **DigitalSign Reader** – an edition not containing “active” features, but allowing opening, displaying and the verifying of electronically signed and time stamped 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.
- **Professional Integrated** – a special edition software distributed by Developer Licensees, designed to be integrated into other applications. Fully supporting the programming interfaces but not containing any user interface.

4. Tables

The following tables demonstrate the tested compatibility of DigitalSign with:

- Several third-party software tools used to display document contents;
- Signature devices
- Timestamping services

Table 4.1 – Integration of DigitalSign 3.0 with software productivity tools

The following table shows integration of DigitalSign 3.0 with some software products used to display in the SecurView environment.

In particular, the table demonstrates for each product: the tested versions, format of documents, references to international standards and/or public specifications and an indication of the security level associated with the usage of each software product as a viewer.

Software used by DigitalSign 3.0 to display documents (1)	Version	File format	Standard ISO and Publicly Available Specification	Security level (2)
CompEd SecurView	2.0	JPG, TIF, WMF, BMP, PCX, PSD, PNG, TGA, EPS, CMP, TXT, RTF, binary (HEX)	JPG (ISO/IEC 10918-4:1999) TIF (ISO 12639:1998) BMP, WMF (www.microsoft.com) PSD, CMP (www.adobe.com) PNG (www.libpng.org/pub/png) TGA (Truevision Inc. Indianapolis)	*****
Adobe Acrobat	4.0, 5.0, 6.0, 7.0	PDF		****
Adobe Acrobat Reader	4.0, 5.0, 6.0, 7.0	PDF		
Microsoft Internet Explorer	4.01 o sup.	HTML	HTML (www.w3.org)	
Microsoft Word	97, 2000, XP, 2003	DOC		***
Microsoft Excel	97, 2000, XP, 2003	XLS		
Microsoft PowerPoint	97, 2000, XP, 2003	PPT		
Other SW products compatible with Microsoft Active Document	--	--		
Other external applications installed on the computer				*

Notes:

- (1) With the exception of CompEd SecurView, the indicated products are NOT included in DigitalSign packages
- (2) A greater number of “*” characters indicates a higher level of security. The listed values are just a rough indication, related to the adopted technology.

Table 4.2 – Signature devices supported by DigitalSign 3.0

DigitalSign 3.0 supports the PKCS#11 standard for interfacing Secure Signature Creation Devices; the standard adopted by all Italian accredited Certification Service Providers.

Because the list of active providers is continuously expanding, each provider is free to adopt different devices and different PKCS#11 interface software products. The actual compatibility of a specific device (and its own PKCS#11 software components) with DigitalSign should be verified by the user.

It should be noted that CompEd makes continuous efforts to ensure DigitalSign compatibility with most all devices available on the market.

The following table shows devices tested by CompEd, listing the issuing Certification Service Provider, the device type and a reference of the PKCS#11 software component.

4.2.1 PKCS#11 interface

Certification Service Provider	Device	PKCS#11 module
Actalis/BNL	Smartcard Gemplus	GemPKCS - gclib.dll
Actalis/BNL	Smartcard Siemens	CardOS - SI_PKCS11.dll
Infocamere	Smartcard IPM (S.N. < 12...)	SysGillo - IPMPki32.dll
Infocamere	Smartcard IPM (S.N. 12...)	SysGillo - IPMPkiLU.dll
Infocamere	Smartcard Siemens (S.N. 14...)	CardOS - CardOS_PKCS11.dll
Infocamere	Smartcard Cryptovision (S.N. 16...)	Cryptovision - cvP11_M4.dll
Infocamere	USB Token Eutron	Eutron - si_pkcs11.dll
Postecom	Smartcard Gemplus	GemPKCS - gclib.dll
Postecom	Smartcard Incrypto	Incrypto - Incryptoki2.dll
IT Telecom	Smartcard IPM	SysGillo - IPMPki32.dll
IT Telecom	Smartcard IPM	SysGillo - IPMPkiLC.dll

Note:

- (1) Tests were conducted under Windows 98, 2000, XP, 2003 environments, in conjunction with the following card readers: Athena ASEdrive IIIe USB, Omikey/Cherry 2020 keyboard/card reader 2020 USB, Omnikey 4000 PCMCIA card reader. Tests were not run under Windows NT4 because such operating system does not support USB card readers
- (2) The usage of a PKCS#11 device takes place by connecting DigitalSign to a software module distributed together with the device itself (normally the Certification Service Provider); such software is not produced by CompEd; compatibility of such software with the hardware and with the operating environment is not under the influence of CompEd in any way. With the table below CompEd aims to provide indications about conditions of positive tests, not excluding that a module is compatible with DigitalSign under different conditions or that the module could show incompatibility under similar conditions.

- (3) When using a PKCS#11 signature device the card reader and its driver (or the driver of an USB token) are interfaced by the PKCS#11 module and not with DigitalSign directly. It is therefore, impossible for CompEd to ensure any compatibility with card readers or even to simply provide a list of compatible readers. In this section CompEd is limited to indicating the readers used for our tests and not excluding that other readers may be compatible. Nor does CompED exclude that the indicated readers may show incompatibility in different environments or contexts.

4.2.2. Direct APDU interface

Some devices are also interfaced at APDU level (not PKCS#11), mainly to be initialized through the Personal Certification Authority of DigitalSign.

A list of devices follows:

Device	Manufacturer	Model	ATR code(1)
Smartcard	Schlumberger	Cryptoflex 8K	3B, 85, 40, 20, 68, 01, 01, 03, 05
			3B, 85, 40, 20, 68, 01, 01, 05, 01
			3B, 95, 15, 40, FF, 68, 01, 02, 01, 01
			3B, 95, 15, 40, FF, 68, 01, 02, 02, 01
			3B, 95, 15, 40, FF, 68, 01, 02, 02, 04
	Gemplus	GPK8000su512	3B, A7, 00, 40, 18, 80, 65, A2, 08, 01, 01, 52

Table 4.3 – Timestamping services supported by DigitalSign 3.0

DigitalSign 3.0 supports standard RFC 3161 for timestamping.

Most of Timestamping Service Providers active in Italy offer a proprietary access mode to their servers, requiring the client's software to interface with the service itself.

The following table shows currently supported services:

Provider	Service	Internet Address	Note
Actalis	Actalis TSA	https://193.203.230.233/test/proxy/proxyTSA.php	
Infocamere	Infocamere TSA	https://www.carm.infocamere.it/carm.dts/ServletDTS	
IT-Telecom	IT Telecom	https://portal.tipki.it/tsservicessslmanagement/servlets	Policy: 1.3.76.12.1.1.2
IT-Telecom	IT Telecom Direct	IP: 62.77.36.36 Port: 318	Policy: 1.3.76.12.1.1.2