SMARTACCESS

SealSign

A complete platform for digital and biometric signature of e-documents

SealSign

SealSign is a modular and scalable digital signature platform that easily integrates with business applications and is accessible from most mobile devices

SMARTACCESS

Benefits

- Reduces costs and improves business processes
  - Contributes to "a paperless office" dematerializing many business processes

- Improves productivity
  - Allows to sign a document anywhere and at anytime using a touchscreens devices (such as smartphones and tablets) and integrates easily with business and productivity applications

A modular and scalable platform

Engine	BioSignature	Central Key Control	eArchive	SignBox	for SharePoint
Advanced digital signature engine	Signature and biometric comparison engine	Centralized custody and management of digital certificates	Long-term storage and custody of electronic documents	Signbook application accessible from web browser and mobile devices	Integration module with Microsoft SharePoint Server

SMARTACCESS

SMARTACCESS

Biometric signature engine and user authentication according to user biometric characteristics

SealSign BioSignature

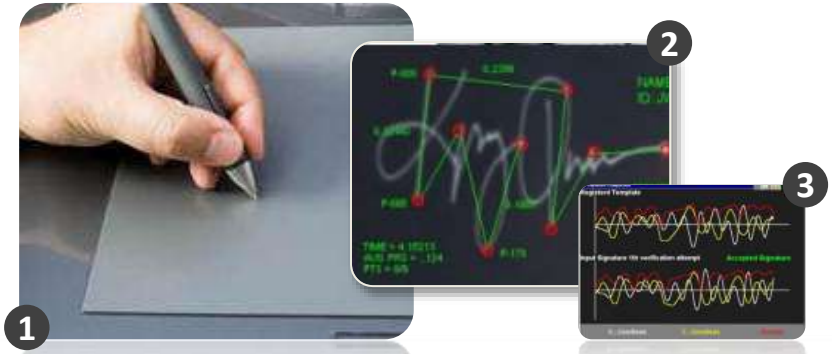
An alternative and universal method to sign electronic documents through the capture of signer's biometrics features and with full legal validity in most regions & countries

The biometric signature

- Any biometric feature that allows that a person transmits his free willingness and consent with a document content could be used to sign a document
- The handwritten signature has been used for centuries for this purpose

The biometric signature

- The signature dynamics is based on the handwritten signature of a person made on a capture device with a touchscreen. During the signing the device records some parameters such as **speed , acceleration, position X and Y and pressure**
- A mathematical algorithm generates a signature calligraphic pattern from these parameters that uniquely identifies the signer



SMARTACCESS

Why should we use the handwritten biometric signature?

- Allows document signature anywhere and at anytime using a touchscreen device
- Broad social acceptance as an authentication method or giving consent over content
- Legal validity of signed documents in most countries

SMARTACCESS

SealSign BioSignature

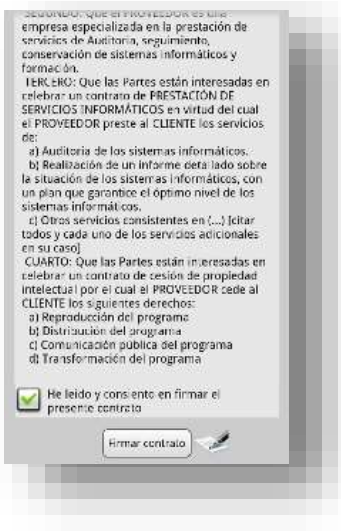
- ✍ Can use as **capture devices** any tablets or smartphones that can capture speed and pressure while the user does hi signature. Samsung Galaxy Note and Samsung Ativ tablets with S Pen are specially recommended.

- ✍ **Web Services based server** that integrates with a digital signature engine with time stamping service

- ✍ Can also perform the **verification of the identity** of the signer by comparing his biometric captured data (signature dynamics) with a stored template in real time

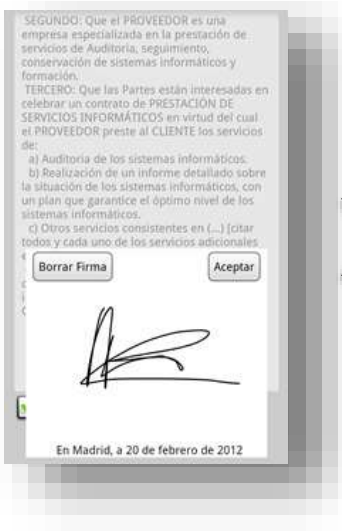
Three easy steps to sign a doc

1



User reads the document and consent to sign it

2



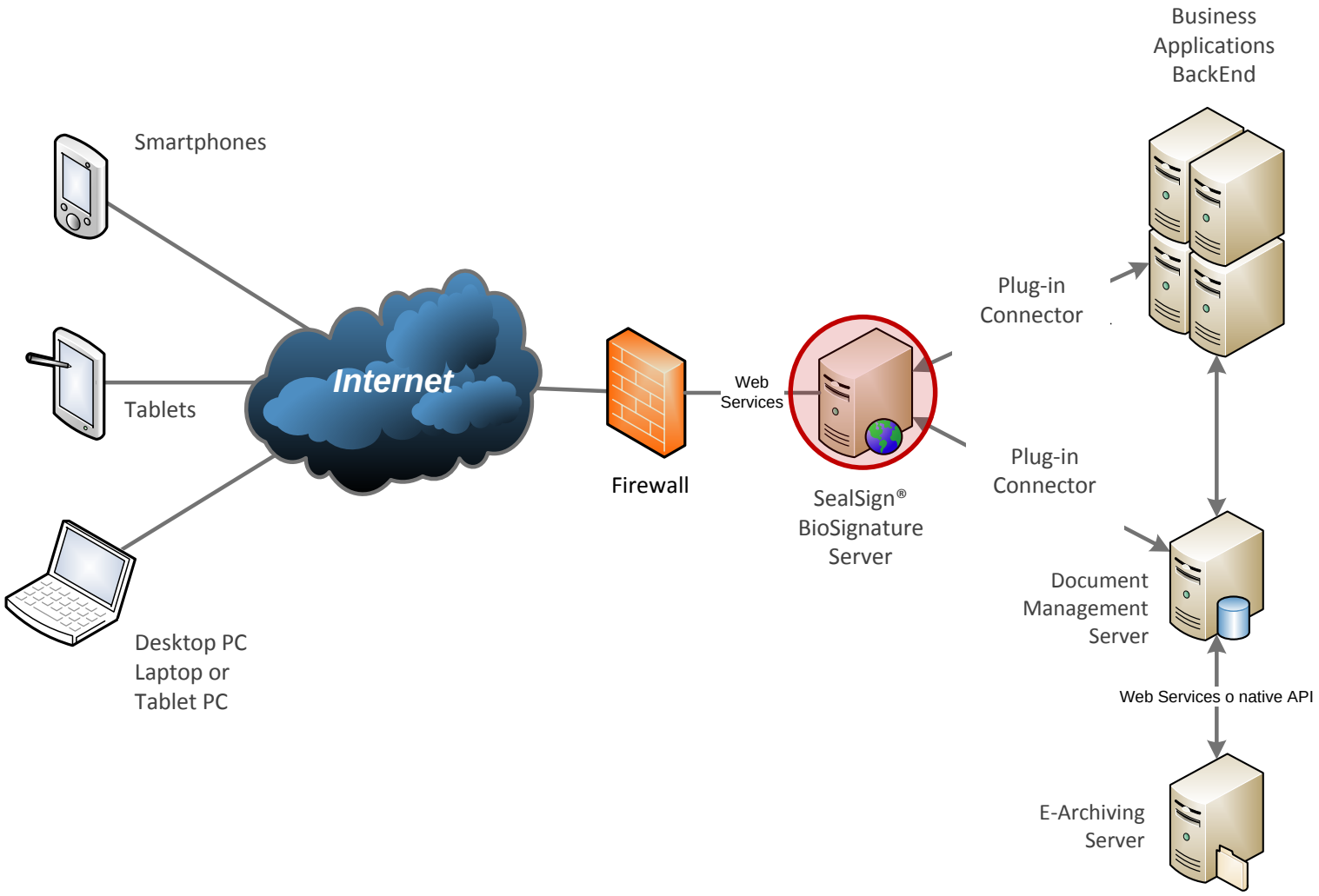
Signs over the touchscreen using his/her handwriting signature

3

Review the signed e-document generated

SMARTACCESS

Solution architecture



Interoperability and standars

SealSign® BioSignature manages biometric information according to
ISO/IEC 19794-7:2007
It allows interoperability with another systems and eliminating vendor dependence

SMARTACCESS

SMARTACCESS

Digital signature server engine

SealSign Engine

A complete digital signature engine that generates advanced electronic signature formats (CAdES, XAdES & PAdES) with validation and timestamp authorities

Signature engine

Flexible

- Centralized and scalable SOA Architecture
- Signing of any type of files (PDF, Office, OpenOffice, XML, Binary)
- Intetration with main devices of HSM, smartcards and tokens

Versatile

- Automatized signature on server
- Signature on PC with multi-browser support
- Signature on mobile devices (Smartphones and Tablets)

Complete

- Implements cooperative signature
- According to the last e-signature standards
- Validation authority
- Time stamping authority

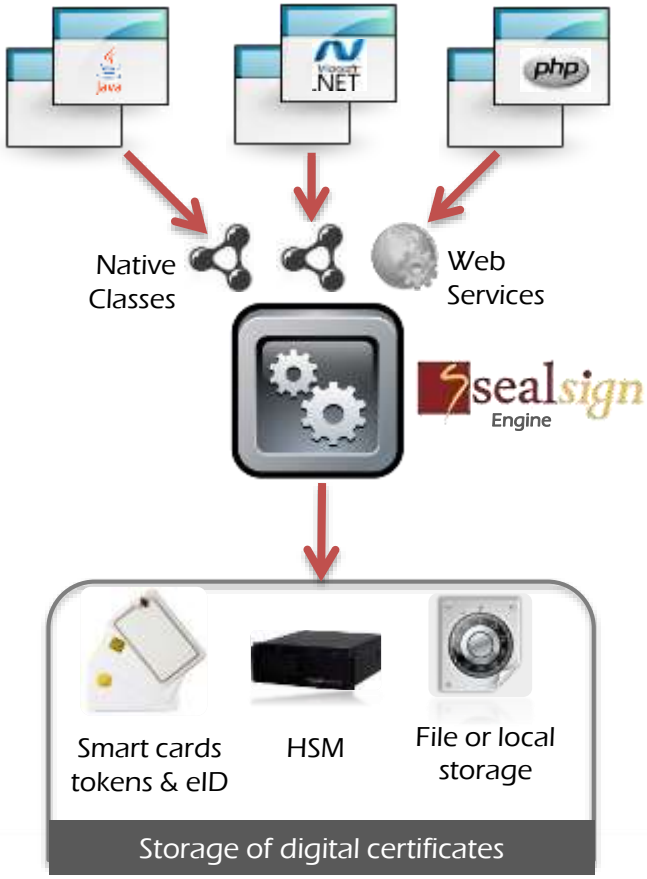
SealSign Engine

Enterprise Server that enables the integration of the electronic signature of e-documents in business applications and mobile devices

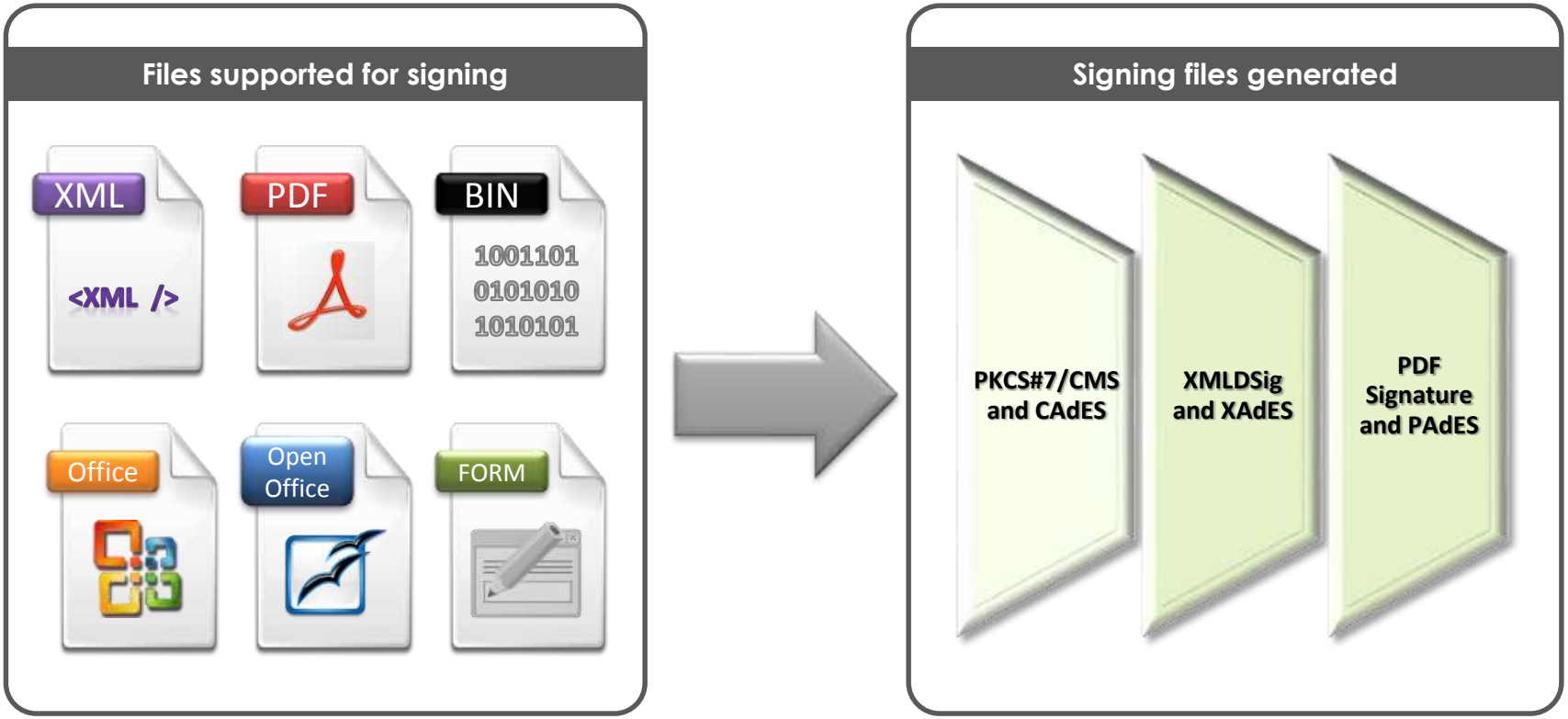
- Web services-based architecture
- Signature of any electronic document format
- Includes a full validation authority (VA) of digital certificates compatible with many PKI providers
- Incorporates a Time Stamping Authority (TSA)
- Allows signature on the move from smartphones and tablets
- Available connectors for integration with business applications and document management
- Server or client signing based on the latest European standards for advanced electronic signature (AdES)
- Secure and interoperable. Compatible with electronic ID cards and other X.509v3 certificates

SMARTACCESS

SOA Architecture



Standars and formats supported



Digital signature engine

Web Services

Automatized signature from applications on server (e.g e-invoicing)

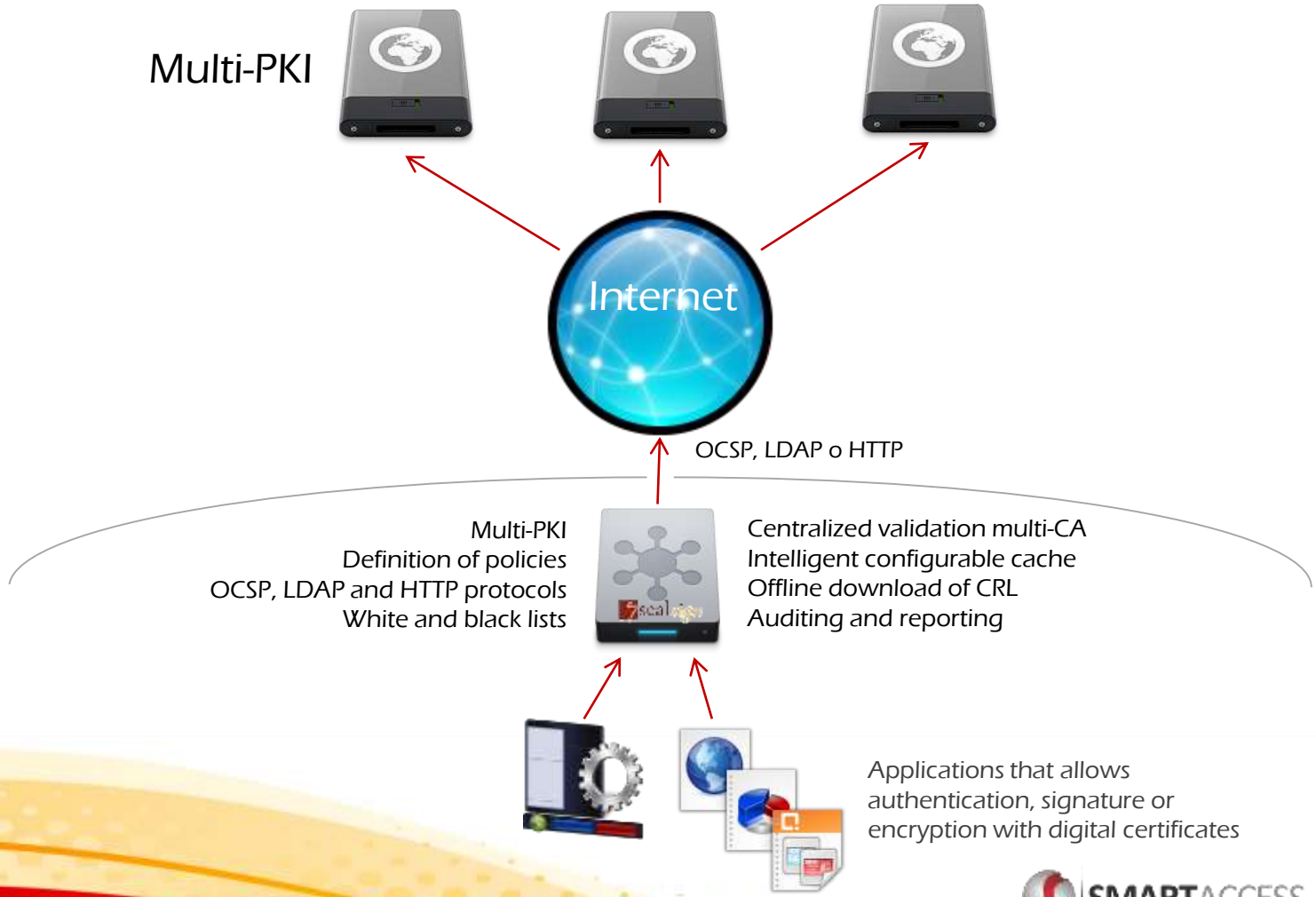
Signature on PC with multibroswer web support

Signature from smartphone and tablets

SMARTACCESS

Validation authority included

Improves efficiency and security



SMARTACCESS

Time stamping in signatures

Generation of long-term signatures using advanced formats

- T, X, XL and A profiles of CAdES and XAdES formats

Allows to use third-party time stamping authorities

- According to IETF RFC 3161
- Through configuration on signature engine

Includes a complete time stamping authority

- According to IETF RFC 3161
- Allows to issue automatically time stamping by installing a TSA certificate

Fundamental element in implementations of electronic invoicing, certified digitalization, document management, Telematic register, etc…

Cooperative signature engine

SealSign Engine implements cooperative signatures by executing on sever the heaviest cryptographic and signature processes, so it releases devices from this work

This feature is useful in scenarios when there is a limited bandwidth i.e. to sign on mobile devices

SMARTACCESS

Compatible with cryptographic hardware

SealSign Engine is compatible with main HSM equipment providers (Hardware Security Module), Smart cards and USB cryptotokens

Smart cards with Microsoft CryptoAPI driver or PKCS#11

USB Tokens with Microsoft CryptoAPI driver or PKCS#11

Hardware Security Module in network appliance format or PCI card

SMARTACCESS

SMARTACCESS

Centralized management of X.590v3 digital certificates.

SealSign Central Key Control

Enables to store and to central manage the corporate and personal digital certificates enforcing the company policies using the module certificate usage policies

SealSign Central Key Control

Allows centralized storage of corporate and personal digital certificates on specialised cryptographic devices and manages the access to them through policies authorizing the usage from certain equipment, applications, URLs and/or users

SMARTACCESS

Main features

Centralized storage of digital certificates on servers, tokens, smartcards or HSM with Active Directory integration

A private space for each user (**virtual smart card**) with their own PIN & PUK

Transparent use of digital certificates from PCs, smartphones and tablets with different strong authentication methods when private keys are used

Integration with SealSign Engine **allows e-docs signature from mobile devices**

Central **auditing and reporting** of the use of the digital certificates

Usage policies

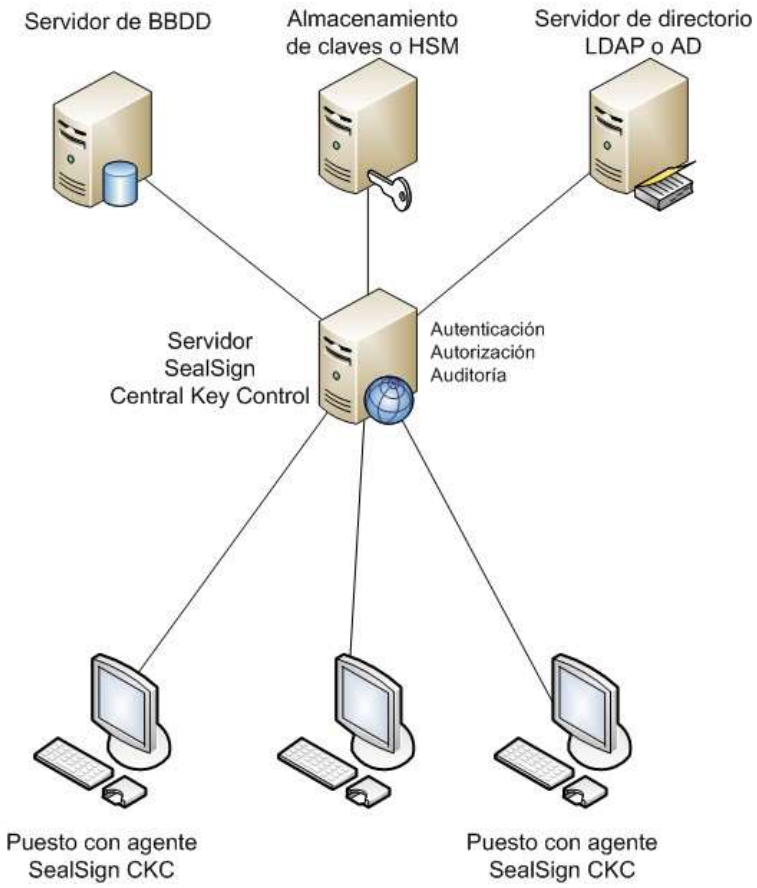
- Possibility of limiting access to each certificate for a group of applications, time periods and/or websites, strengthening access security
- Some combinations of these access conditions:
  - Authorized users (either locals or belonging to the organization's Active Directory)
  - Equipment from which access is permitted
  - Authorized applications
  - Authorized URLs (only on Internet Explorer)
  - Authorized periods of time

Benefits

- Improve security on custody of certificates' private
- Allows users mobility between different organisation's equipment and maintains access to the certificates
- Complete traceability of using of organisation's digital certificates
- Possibility of high availability configuration

SMARTACCESS

Architecture



SMARTACCESS

SMARTACCESS

Securing Electronic Historic Archive

SealSign eArchive

Long-term storage of electronic documents and guarantee of confidentiality and integrity of the safeguarded documents

SealSign eArchive

Long-term storage and custody

of electronic documents through the application of access, retention and resigning policies

SMARTACCESS

Why is eArchive necessary?

- Allows the **storage and custody of the company's e-documents, as dictated by law**, for long periods of time, **guaranteeing the integrity** of such, limiting and **monitoring access** to such and **generating electronic evidence** if required
- Constant **increase of computing power** of computers threats actual cryptographic systems
  - A signature algorithm based in a secure key at this moment, won't be secure in 5 a10 years timeframe.
- Includes **mechanisms that guarantee integrity, confidentiality and inalterability of the documents** (in case of legal dispute)

SMARTACCESS

Policies applicable to the documents

Retention policies

Establishes the period of time that a document remains in custody on the platform

The document is identified, encrypted and resigned when it is incorporated to the platform

This document is destroyed securely once the established period has elapsed

Resigning policies

The documents are stored in containers encrypted with the AES-256 algorithm and the

frequency with which automatic resigning

(XAdES-A format with time stamping) of the

safeguarded documents will take place is

established. The latest secure cryptographic

algorithm is always applied

Access control policies

Access restricted to authorised persons

Policy and traceability of all access to a document

Encryption of documents and different security mechanisms of containers prevent the manipulation of the documents outside the platform

Main features

- SealSign eArchive
  - SOA architecture based on web services makes easier the integration with business applications and document management
  - Allows the custody of any type of (text, PDF, images, binary, etc.)
  - Creation of archive volumes with strong encryption (AES-256) of up to 250 TB
  - Capable of incorporating metadata with each document
  - Unique identification of each document incorporated
  - Auditing and detailed reports in relation to activity and access to documents