SOLUTION GUIDE

Serban Biometrics | intel | hp | Microsoft

BIOMETRIC SIGNATURE SOLUTION GUIDE FOR FINANCIAL SECTOR

Optimizing business processes through mobility

>

An Evolving Sector

The financial market is constantly evolving. The reduction in the number of offices due to the consolidation of organizations **(36% since 2008)**[1] as well as the optimization of their resources and the increase in the productivity of their employees are forcing the industry to transform its work methodology, turning their managers into mobile offices.

The acceptance and signing of agreements and contracts between the financial institutions and the customers via physical documents was one of the obstacles that hindered the quick processing of documentation that banks were looking for, in order to give their customers a better service and reduce the cost of business opportunities.

Contract processes produce a huge volume of documentation, which must be sent, signed and filed, resulting in loss of time and use of physical space.

On the other hand, mobile technologies provide the possibility of optimizing those processes that currently take place in bank branches, so they can now be carried out anywhere at any time.

To do so it is essential to be backed up by a solid and reliable technical solution, which enables quickness, mobility and cost saving.

What is a Biometric Signature?

The term biometry refers to those technologies based on the recognition of some physical and non-transferrable characteristics in each person with the purpose of their authentication and identification.

The basic characteristics a biometric recognition system must comply with are:

1. **Performance**: this characteristic refers to the accuracy, rapidity and reliability achieved by the biometric system in the identification of individuals.
2. **Acceptability**: it shows the degree to which people are willing to accept the biometric system in their daily lives.
3. **Reliability**: this characteristic demonstrates how difficult it is to challenge the system.

The **Biometric Signature** is the technology that enables the graphological patterns of the hand-written signature to be captured by means of devices especially designed for this purpose, such as pads, digitizing tablets and active pens.

These devices, together with a mechanism to generate electronic signatures and capture the image of each signature, are able to recognize and capture its biometric pattern, which is individually specific for each human being.

The biometric features mainly take into account the speed and acceleration of the writing, the pressure applied on the surface by signing, the changes in direction and the movements of the pen. It enhance the confidence that the signature genuine and is not forged.

Biometric Signatures vs Digital Signatures
Two complementary signature solutions.

The **Digital Signature** is a type of electronic signature which, by means of a cryptographic mechanism or a long number code assigned to a person, gives an electronic document authenticity and acceptability due to the capture and recognition of his/her signature image.

The digital signature is usually kept on a computer or, in some cases, on a card. It must be remembered that the digital signatures are only as safe as the means by which they are kept (phone, card, etc.), which can be stolen, lost, damaged, etc.

Therefore, the use of a digital signature does not always guarantee the correct identity of the issuer.

The **Biometric Signature** captures and recognizes the image of the signature itself as well as the biometric **pattern** of the signer's graph, as detailed above. These patterns are exclusive to each person.

Besides the graphic aspects of the image of the signature, the framework of the **Biometric Signature** includes real-time **graphometric information** obtained from a device especially designed for this purpose and associated with the signature system, linking it to the document and the signer permanently and cyphering such information so that nobody can manipulate it.

The biometric signature represents the ideal bridge between the conventional and recognized signature on a document and the necessity for electronic documents to be recognized only by individuals. This application offers the intervening parties the maximum security and control over documents originating from, negotiated through and stored in a digital domain.

Combined Biometric Technologies

Using biometry ensures the person's authenticity when interacting with a capture device: fingerprint reader, iris reader, type register, signature register, etc, as it is all about the person's essential characteristics.

However, due to changes in the capture scenes (type of device, place in which it is located, ambient lighting, noise, etc), there are distortions in the captured data, which generate false negatives, provoking uneasiness in the user and misgiving in the service provider.

In order to avoid these situations, it is recommended that two or more captured biometric factors for the same act of authentication/identification is used.

By using two or more biometric factors significantly enhance the reliability of biometric authentication.

At the moment technologies based on biometry are available in devices frequently used by customers and users, such as Smartphones, personal computers, laptops and tablets. The advantage of using combined biometric technologies is that they ensure **strong authentication**, necessary in the case of unattended remote signatures.

CHALLENGES FOR THE FINANCIAL INDUSTRY

One of the challenges the financial market faces at the moment is the **optimization of processes** in the acceptance of paper documentation by the customers, such as quotations, authorizations, contracts, bills, opening of new accounts, etc.

All these processes generate an enormous volume of documentation that must be signed, sent and filed by the organizations.

Time, security, physical space and a better service for customers make these processes a key area that can be optimized by changing the way companies work.

Most financial institutions are seeking faster and more reliable technologies that make their businesses more efficient and productive, in keeping with the demands of the market and the needs of their customers.

Similarly, cost control in the processing of physical documents and time saving when institutions and customers deal with such documents is another one of the key challenges are facing banks today and in the future.

On the other hand, their customers, covered by data protection regulations, demand greater security in risk management control, both in physical and virtual documents.

Cases of Use

The Biometric Signature is an excellent system for identifying people, which is used in many processes due to two main reasons: **security** and **convenience**.

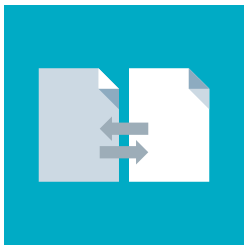
The Biometric Signature solution on mobile devices has become a key item in the processing of documents between the bank and its customers, providing savings in paper costs, logistics, space and time and offering a much higher level of security than it was previously possible. If we add the **mobility** factor, the solution encourages proactivity and reduces the costs of business opportunities, saving customers unnecessary journeys.

Approximately **90%** of financial institutions already have a biometric signature solution, but only **20%** of them have the same solution on mobile devices[2].

In the case of insurance companies, **10%** have a biometric signature solution, but less than **1%** of them have a solution on mobile devices[3].

Due to its singularity, permanence, universality, acceptability and performance, the Biometric Signature has become a technology that is widely used across the financial sector and by insurance companies:

- **Signing of bank credits**: where the customer's signature is essential, both in the credit contract and in the insurance associated with it: Life, Home, etc.
- **Personal Credits**: as in the case of mortgage loans, the signature is compulsory in both the contract and the associated insurance.
- **Opening an account**: the Biometric Signature substitutes the old records where the signature was registered and limited exclusively to the bank branch.



- **Credit card applications**: where the signature is compulsory, both in the application and the withdrawal of the card.
- **Signing of insurance policies**: the customer signs the contract on the mobile device in front of the agent, saving the journey to the insurance office and the delivery of contracts in paper format.
- **Acceptance of work due to an accident**: where the worker, once all the tasks are finished, requires the signature of the customer on the work order.
- **Cancellation of policies**: Policy cancellation orders, without the customer having to travel or send the order.
- **Payment with medical assistance cards**: as an acceptance of the invoice, that will later be charged to the insurance company.
- **Appraisals**: mainly in accident appraisals, in order to avoid subsequent claims from both parties.

Mobility + agility = productivity.

The transition towards mobility that companies want to implement often required the use of different devices, depending on how and where work is carried out. Today, however, mobile devices based on Intel processors have been designed to satisfy the users' need for mobility and companies' security requirements.

Touchscreen devices have redefined the way we interact with technology, from a small tablet to an **AIO** (all-in-one PC), allowing a company's professional staff to meet around one single screen in a more natural way of interacting.

On the other hand, today's office workers still need a traditional keyboard and mouse to create, present and collaborate. **2 in 1 devices** incorporate all the necessary elements in a thin, powerful, easy-to-carry gadget.

The 2-in-1 devices (equipped with either Intel® Core M processors or Intel® Atom™ processors) provide new transport and usage facilities for mobile workers at worksites, with:

- Designs for lighter, ultra-slim appliances than ever, since they have no ventilator – a first for this type of device.
- The maximum versatility on the move, thanks to the easy switchover from keyboard to touchscreen with a simple-to-use detachable. The powerful productivity of the laptop is thus combined with the ergonomic assets of the tablet, optimizing efficiency and flexibility according to the needs of the moment.

Today the workstation can leave the office and a manager can sign the required documentation both in office and at the customer's location. This acceptance process results in the elimination of huge amounts of paper documents and the optimization of managers' productivity. The document never resides in the mobile device always resides in the server.

Using mobile devices as the new tool.
The relationship between manager and customer has been transformed significantly the by the use of next generation mobile devices.

Mobile devices offer Banks and Insurance Companies the possibility of transforming the fixed office approach. Currently, customers must suffer long queues and be attended to at a fixed workstation. Using mobile devices, customers can be attended to anywhere in the branch or in a private office, where employee and customer are able to interact in a more personal way.

Let's take as an example the "sales process of an insurance policy": the insurance company introduces the product to the customer by different means (phone, advertising or through a company representative who travels to the customer's home to explain the characteristics of the product). Once the customer has shown interest in a certain product, the insurance company delivers the relevant documentation and contract to the customer (usually by post) so that he/she can accept the conditions by signing several copies: two for the company and one for the customer. The two copies for the company must be signed and returned by post.

Afterwards the insurance company must check the documentation and file it for safekeeping.

Using the Biometric Signature on a mobile device, all the stages described in the above paragraph could have been reduced to a single step, anywhere and at any time.

Customers' perceptions change positively as they receive a better service and associate the company with technological innovation and modernity.

*The proposed solution consists of the application of biometric signature recognition "**BeSign**" **(Serban Biometrics)**, combined with the mobile devices **Elite* X2 1011** and **Elite Pad*1000**, by **Hewlett Packard* (HP*)**, and the functionality of security and integrated management capacity of the Intel technology on the **Windows* 8 of Microsoft*** Operating System.*

The main characteristics of the **BeSign** solution are:

- **Multichannel**. This allows an e-document to be signed in various legally acceptable ways: by digital certificate, e-DNI, bank keys card, OTPs, online banking (PIN + OTP in the mobile), digital signature, etc.
- **BeSign** can be applied to both mobile and fixed-line environments and is supported by several platforms: Java*, Linux*, Microsoft, iOS*, Android*.
- It is also **compatible** with Citrix* virtual environments. Unique development for the data exchange channel between server and customer **ICA** (Independent Computing Architecture) by CITRIX.
- **Encryption systems AES 246 and RSA 2048**.
- There is a **yearly audit** carried out by Legal Auditors (Bercovitz-Carvajal Office) and a Security Audit at code level for **S21Sec**.
- **Legal compliance**:
  - **AES 246 and RSA 2048** (Security).
  - **ISO32000-1** (Exchange and display of long-standing documents).
  - **ISO/IEC 19794-7** (Standard of coding and storage of biometric information).
- **Sealing and encrypting** of the signature in each signed document, without the possibility to remove it for use in other documents. Each signature is univocally linked to a document.
- Within the framework of the functionalities of the proposed solution and in order to provide the maximum security, "**Serban Biometrics**" offers the possibility of using a combined group of biometric technologies called "**BeBiometrics**".

Components of the solution

The required elements for the implementation of a biometric signature solution are:

- **Application of biometric signature recognition**, with capacity for:
  - Registration of biometric signature to add customer.
  - Recognition of the biometric graph patterns.
  - Signature discriminator.
  - Verification of biometric patterns.
  - Security and legal certification.
  - Process automation.
- **Mobile devices** with capacity for biometric signature recognition and integrated security systems.
- **Operating System**, with biometric recognition systems usable for the development of applications through the API (Application Programming Interface) within a Biometric framework.

Application definition: Functionalities and processes.

The process of biometric signature recognition starts with the **registering of the customer's details** in the bank's system. This process happens only once, when the customer is added to the system. In addition to general details, the customer registers his/her signature on a device that is able to recognize biometric signatures. All this information is stored in the bank's central data base.

When the customer is required to sign a document, the process consists of the following steps:

1. **Document request**: the document to be signed is requested via the mobile device and will be obtained in PDF format linked to a Hash (algorithm that produces an alphanumeric value, often with a fixed length, which represents a summary of all the information given). All the information contained is clearly specified, in a way that can be easily understood by any user: who must sign, in which order and where the signatures must go (coordinates). The document is displayed on the device through an XML file (standard electronic file to exchange information).

2. **The document is sent to the signature system**: in this process a square appears with a space reserved for the signature. If one single bit of the original document is modified, the hash will also change.

3. **Capture of the Biometric Pattern**: when the intervening parties sign the document, the mobile device is able to recognize the pressure, acceleration, speed and vertical and horizontal movements carried out on the template; it even recognizes the pen's movements when the signature consists of discontinuous strokes.

4. **Timestamp**: the signature is linked to the document as soon as it is signed. The Timestamp is an online mechanism, which can be used to prove that some data existed and has not been modified since a certain moment in time, so that the signatures are linked to document in the exact moment it is signed. Through the verification of the signature in real time (**inclusion of time stamping**) and the **geolocation**, more control over the signer is gained, thus avoiding attempted fraud, identity theft or repudiation or denial of a previously signed document; at the same time, it enables the bank to better control the signing processes and to store the strokes of the signature. The **timestamping** can be given by the application server or can be inserted by a **trusted third party**, giving add value to the document.

5. **All the information is contained in a PDF/A document as Metadata**. The elements of this document are: the contents, encrypted attachments, signatures with their characteristics, etc. All this is encoded using a **public-key encryption** provided in the moment the information is sent.

6. **The PDF/A document is sealed with a bank's digital certificate**, which proves the **integrity** of the document. The biometric signature makes it impossible to manipulate the signed document, thus ensuring the **authenticity** of the signature used by the persons and entities intervening in the exchange of information, as well as the **confidentiality of the data**, as only the issuer and the recipient can see the information contained. The signing of the document may be internal, i.e., with a company certificate or self-generated by the entity itself; or for giving more value and additional security to document this signature can be performed by a trusted third party.

The document and the passwords are stored is given to a **trusted third party** for safekeeping (independent entity that endorses the authenticity of the signature), which acts as a custodian of the documents' encryption and sealing keys. Depending on the risk of the operation (determined by the financial institution), the trusted third party inserts a timestamping to increase the assurance level to the signed document.

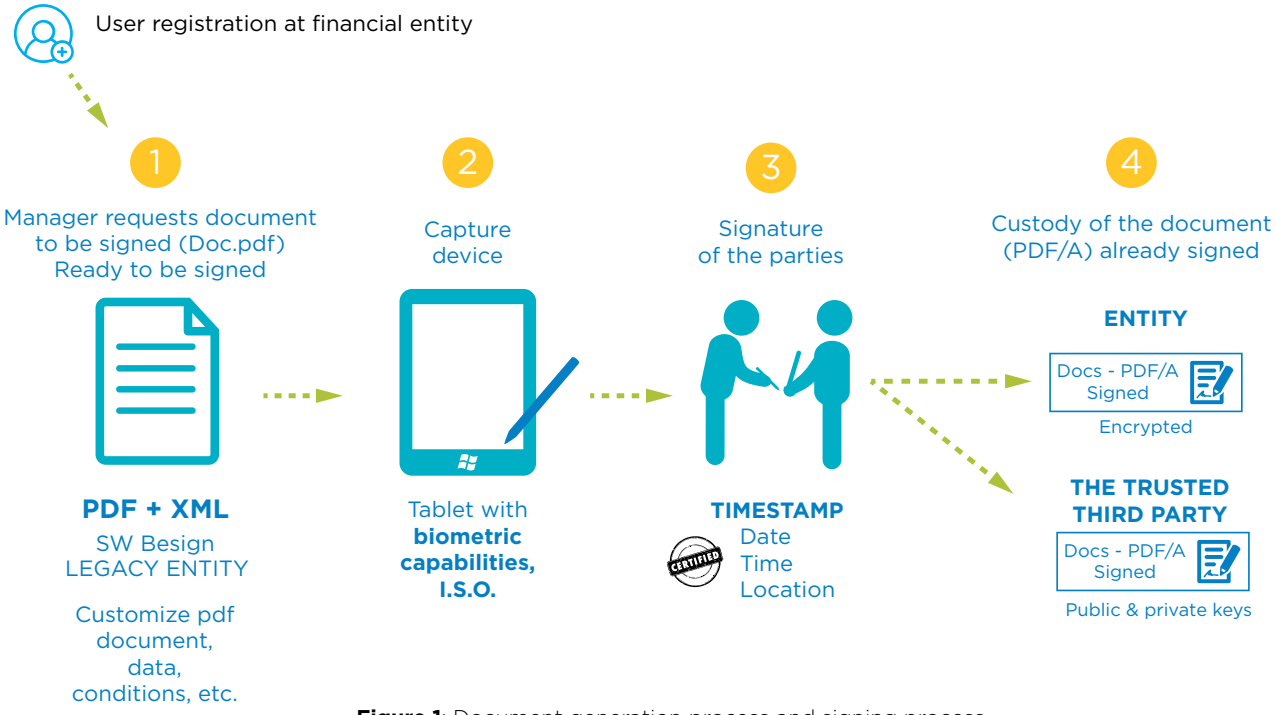


Figure 1: Document generation process and signing process.

Verification process (in the case of repudiation)
If **verification for rejection or repudiation by one of the intervening parties** is necessary, the system the system compares the signature of the document against those indubitable signatures to be collected at the time of litigation. The **trusted third party** is the only one that possesses the keys to decipher the document; therefore this entity becomes highly relevant in the **verification** process.

The trusted third party, also called **Trusted Mediator**, is an approved and neutral entity, which acts as a "**Digital Notary**".

Once the document has been decrypted, the process is quite simple, as only two samples need to be compared, with a positive or negative result.

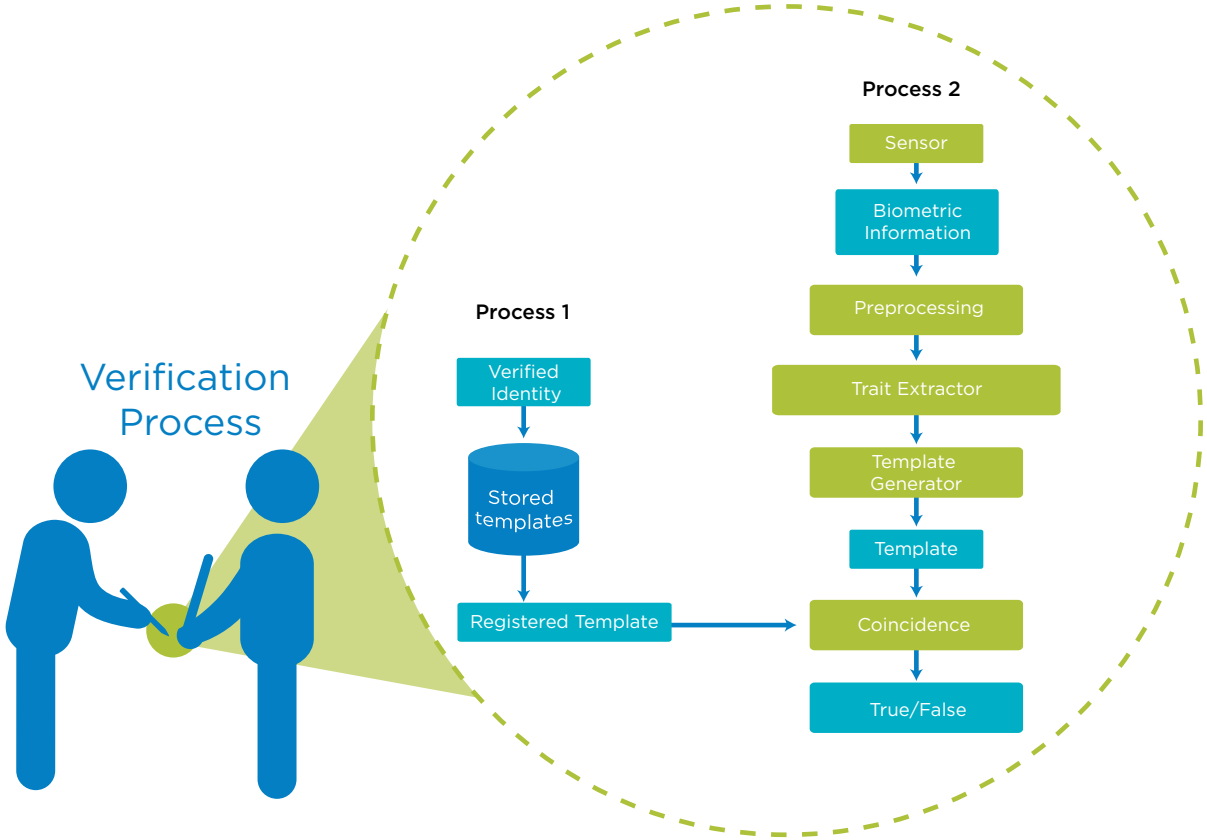


Figure 2: signature verification process (in case of repudiation).

Description of the devices Mobile devices, Capacities of biometric signature capture.
The devices required for the Biometric Signature are: digitized tablets connected to personal computers and generalist tablets, preferably able to register the strokes and all other aspects of a written signature and equipped with pressure-sensitive technology.

The detachable devices (2 in 1) **HP Elite X2 1011** and the tablets **HP Elite Pad 1000** stand out among the mobile devices approved for the biometric signature solution, with Intel Core M and Intel Atom processor Z2795 respectively.

Due to their characteristics and features, these two devices have become the most suitable solution for working in both an office and mobile environment. It is worth highlighting their versatility, easy handling and lightness. A laptop and a tablet integrated in one device; just by sliding the screen, the laptop becomes a tablet.

Depending on the biometric capture technology that each mobile device has, the use of a pencil able to detect the pressure, speed and movement applied when signing may be required.

Multichannel solution – Ways and methods of signing using different devices and channels
The **BeSign** biometric signature solution is **multichannel** and accepts various types of identification and signature with complete integration of the signed document using different products, irrespective of the devices and means used in the execution of deferred signatures or multi-signatures.

BeSign has been adapted to different architectures, systems and channels allowing the signing of the document through other signature channels in order to be used in most environments where signature recognition and identification is required:

- Environments where the signature is required through a device able to recognize **biometric signatures**.
- Through a keyboard where identification is requested with a **coordinates card**.
- In procedures where the use of a **digital certificate** is required.
- In cases of identification which require a **code** or **token** through a keyboard.
- **Electronic ID**.

Figure 3: Different identifying channels accepted by BeSign.

Legal Validity. Authenticity of Signatures and trustworthiness of documents.
The biometric signature as an element of identification complies with the three requirements by law: **Authentication, Trustworthiness** and **Non-repudiation**, which means to authenticate and confirm irrefutably the author of the signature, proves the trustworthiness of the biometric data and the signed document and give **legal validity** due to the unique link to the signer.

There is no specific regulation regarding the validity of the Biometric Signature. However, from a legal perspective an advanced system of electronic signature –which applies biometric technologies solutions- might be used to create digital signatures that have the same legal capacity as the handwritten signature on paper, according to the **article 5.1** of the European Directive on Electronic Signatures. This is because both will be governed by the general rules of **Evidence**".

Nowadays the normalization of the processes of legal certification is covered by the rulings of the "***Superintendencia de Banca y Seguros***" (Banking and Insurance Commission). Their decisions are revised every two years, depending on the evolution of the technology.

On the other hand, the Biometric Signature is compatible with the new law on electronic signatures, as can be verified by the latest draft of the European Regulation "Electronic identification and services of trust for electronic transactions in the internal market".

According to recent publications, the legal security of the advanced signature must revolve around **10 basic principles**:

1. Capture of dynamic biometric elements of the signature linked to its production data.
2. Univocal connection between the biometric elements with the signed document.
3. Impossibility of inserting the signature in other documents.
4. Trustworthiness of the signed documents.
5. Authenticity of the document and link with the signer.
6. Confidentiality of the biometric data and protection of the information, in compliance with the **LOPD** (Organic Law on the Protection of Data).
7. Enable the legal owner to check the signature biometrically.
8. Possibility of proving the validity and univocal link of the signature in a litigation process.
9. Probative symmetry.
10. Long-lasting format.

Biometric Signature solution BeSign complies with all the requirements established by the European Directive in its definition of Electronic Signature.

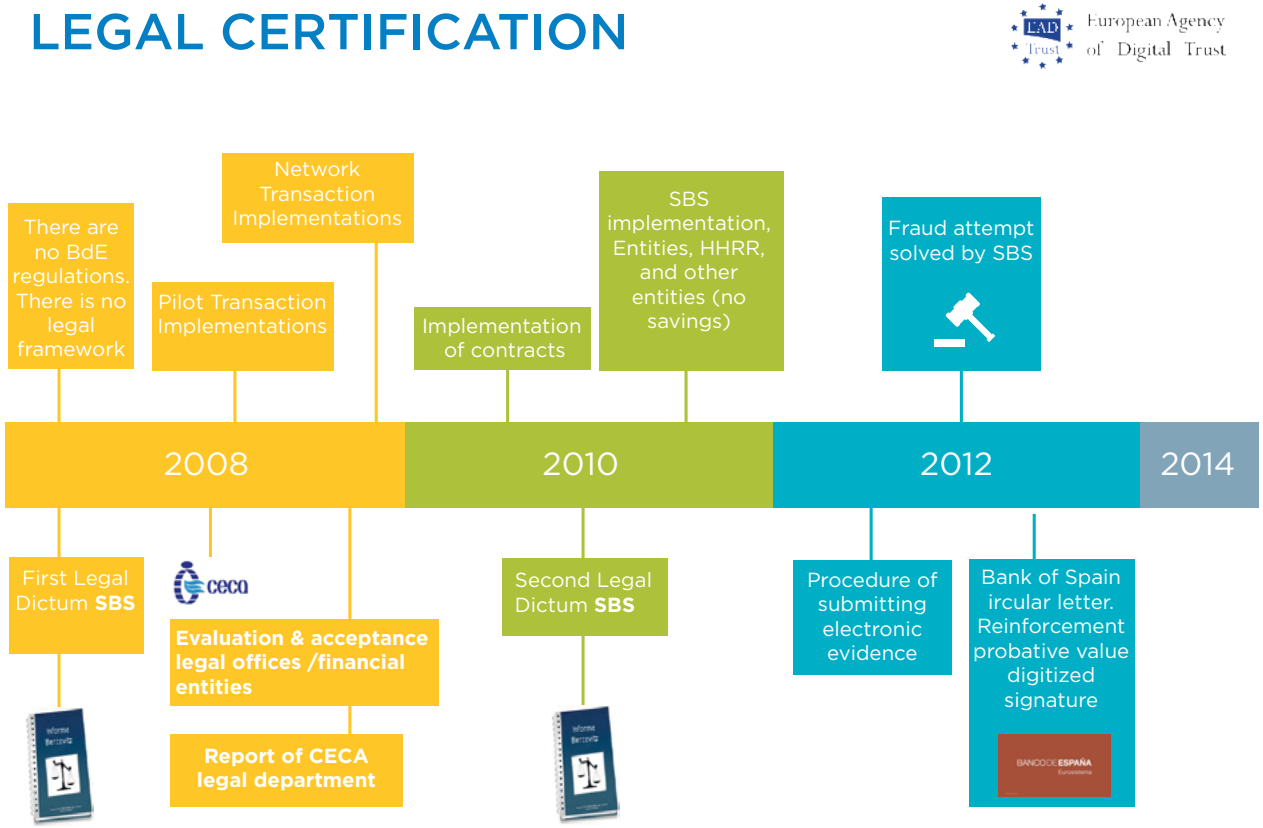


Figure 4: Legal Certification.

Relevant biometric signature regulations and milestones.

Key facts:

- **10 million customers** used some kind of biometric signature during 2012.
- **200 million** operations were carried out during 2012.
- In 2014 this figure rose to **850 million** operations.
- Of these **850 million** operations only **37 cases** were revised due to repudiation and only one came to trial.

There are some signature recognition solutions available in the market offering different levels of performance. However, in order to implement the most complete, intelligent and safest solution we must take into account a series of factors:

Application: the application must meet all the customers' expectations and requirements. The automation of processes, security systems, signature recognition parameters, the design to work in a Web or virtual environment and the integration with corporative systems become specially relevant for a successful solution. The stability and reliability of the application gives the person in charge of the IT department a greater feeling of security.

The correct performance and capacity of a system of Biometric Signature recognition can be assessed by means of a series of **rates of traceability**.

Operating System: companies are very reluctant to take risks regarding Operating System platforms. They look for a solid, agile Operating System with a generalized business implementation, which ensures a long life cycle and has a high integration capacity with the base currently installed.

Although many organizations are also considering alternative mobile platforms, such as iOS or Android, when defining their mobility strategy, Windows users remain very committed to its platforms. Features such as the stability and security of the platform, its easy integration with corporative systems, the management infrastructure and compatibility of existing applications

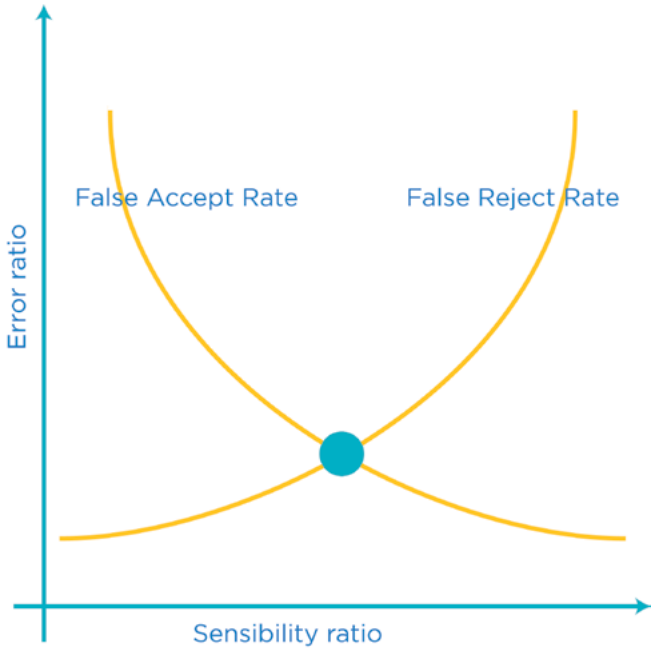


Figure 5: Level of effectiveness of a biometric identification and verification system.

have led to the use of Windows as the operating system for the most relevant mobile solutions in the market. Windows solutions for first-line mobile applications are generally used and make up the common platform for most of the relevant business applications.

Companies contemplate the implementation of mobile tools as an opportunity, as any operation where the customer's participation is required to accept or sign a document can now be carried out anywhere, at any moment and on a light and sturdy device. For that purpose companies are looking for robust, secure, reliable mobile devices that can offer stability, autonomy and a long life cycle.

Mobile devices are exceptionally powerful tools for business optimization. Most senior executives in companies think mobility will affect their business positively.

Choosing the most suitable mobile device is a key piece in the implementation of the biometric signature solution. In order to make a successful decision there are some important factors to take into account:

- The mobile device must be equipped with cutting edge technology. High performance with minimum consumption in order to maximize mobility to the full.
- Financial departments look for a quick **return of their investment**. Therefore, mobile devices must combine high performance and a long life cycle with low maintenance costs, besides also significantly increasing employees' productivity.
- Reduce the number of additional accessories surrounding the mobile device. The device must include everything managers require to do their job properly.
- It is also very important that the devices can be perfectly integrated into the company's existing IT environment.
- The chosen mobile device must have not only a touchscreen, but also the capacity to capture and store biometric factors, such as the speed, the pressure and the time the pen stays in the air between strokes.

Mobile devices can incorporate different types of technology to capture biometric signatures:

- **EMR** (Wacom*): Magnetic Resonance technology, which combines fine sensors, sophisticated algorithms and high-speed data transmission. Wacom technology is made up of three layers: one to detect fingers, another for the LCD screen and a third ERM detection layer (**Magnetic Resonance**) that detects the pen's electromagnetic emission of the pen. This is the technology incorporated in **HP Elite X2 1011** devices.
  As this technology is based in the screen of the device it does not need to be powered by batteries.
- **Ntrig Active Pen technology**: this technology has two layers: the first for detecting fingers and the active pen and a second LCD layer. It incorporates configurable buttons and exchangeable pen tips. It is supplied by a battery that must be replaced once exhausted.
- **Synaptics* –** Active Pen technology that communicates with the tablet through Bluetooth* technology. It incorporates a series of buttons,

which allows the user to take full advantage of the Windows 8 Operating System. The pen incorporates a battery that must be replaced when exhausted.

- **Atmel* MaxStylus*** Active Pen Technology. This incorporates a sensor that detects 256 different levels of pressure and technology to reject the palm of the hand, in order to avoid erroneous data appearing on the screen. It is battery powered.

The factors and requirements described above can be fully met by mobile devices equipped with Intel Core M processors and Intel Atom processors.

Intel® Architecture.

Designed specifically for the latest Windows 8.1 tablets, the Intel Atom processor Z3700 Series delivers excellent performance with four processing cores and Intel® HD Graphics with Intel® Clear Video HD Technology. The energy-efficient system-on-chip (SoC) design helps conserve battery power and enables thin and light designs.

The HP Elite Pad 1000 tablet incorporates the Intel Atom processor Z3795, certified for the 64-bit Connected Stand-By Windows 8.1 64-bit version version. In addition to improved performance and a better user experience with the devices, the 64-bit support prevents those organizations which have fully completed the migration to an 64-bit environment from using the same versions of applications in the HP1000 environment as in the other devices, and reduces the number and complexity of images in the image management of the operating system in Windows environment.

The recommended **HP Elite X2 1011** features Intel core M processor. The Intel Core M processors deliver significant performance advancements, including vastly improved graphics and battery life, in lightweight razor thin designs. New enhancements include:

- An energy efficient design combined with 14nm manufacturing technology enables a 60% reduction in the thermal design point (TDP) allowing thinner, quieter, fan-less designs.
- A new multichip package that is almost 50% smaller in size than the 4th Generation Intel® Core™ processors (Y series) allowing even smaller platform designs.
- The new low energy consumption processor delivers faster processor performance and better graphics performance compared to previous generations.

The new 2 in 1 mobile devices with Intel Core M processor offer everything in one single pack: a multipurpose laptop and a tablet. They are designed for professionals who demand the highest performance and a variety of uses from their devices, to both consult and create content, or even to act as a desktop substitute.

Intel® Wireless Docking technology –incorporated in HP Elite X2 1011 devices- adds a significant innovation in the transition towards a wireless environment, and incorporates the concept of a mobile device to the area of personal productivity.

Intel® Wireless Docking, enabled through Intel® Wireless Gigabit technology, offers simple, seamless mobile-to-desktop auto-docking, which allows instant connection to monitors, keyboards, and printers wirelessly.

Finally, Intel Core M and Intel Atom processors Z3795 incorporate the Intel® Identify Protection Technology (Intel® IPT) that enables the use of strong authentication solutions (Second Factor Authentication), management of digital certificates and protection of transactions, both based on hardware.

Identity theft is a growing global concern for individuals and businesses. Secure, but simple-to-use solutions are required as hackers devise new methods for obtaining usernames and passwords.

With Intel IPT enabled on 2 in 1 and tablet devices Intel provides a hardware root of trust that can be utilized by multi-factor authentication solutions. Intel IPT enabled systems with Intel Core and Intel Atom processors offer additional identity protection and transaction verification methods than can help organizations to implement robust, strong authentication and identity protection solutions.

- Intel IPT utilizes a One-Time Password (OTP) - a unique, one-time use, six-digit number generated every 30 seconds from an embedded chipset that is tamper-proof - enabling seamless two-factor authentication and secure VPN access.
- Intel IPT with protected transaction display (PTD) protects and hides PC display from malware scrapping and proves human presence at PC by first creating a secure PIN input prior to the release of credentials and creating a window that cannot be viewed by a hacker.

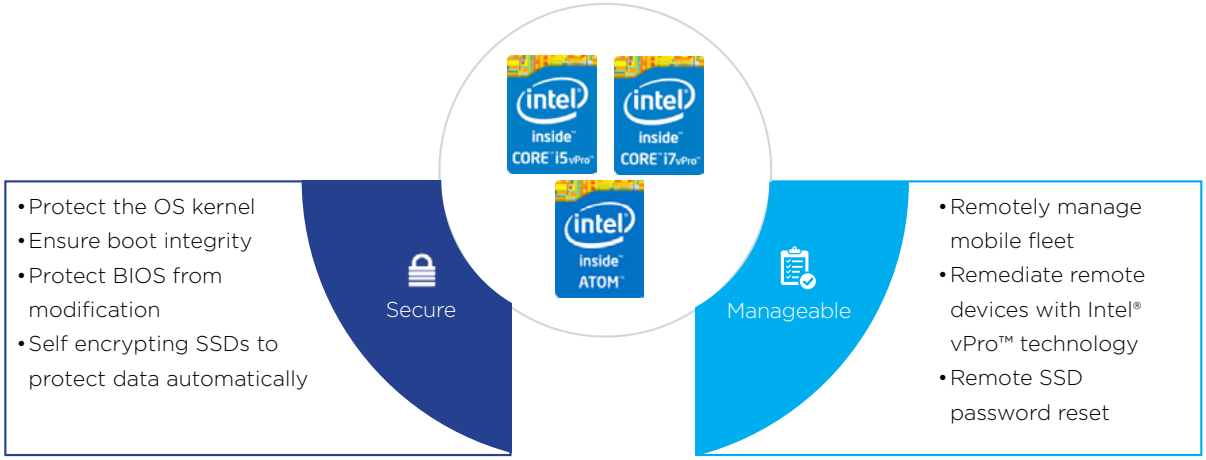


Figure 6: security and management capabilities of Intel processors.

- Users can connect to an Intel® IPT with NFC-enabled merchant or payment site, pay for a product by tapping their NFC-enabled credit card against an NFC sensor on the computer, and complete the transaction with positive identity authentication by Intel IPT.
- Intel IPT with PKI uses the Intel Management Engine to provide a hardware-based security solution similar to that of other hardware security modules like Smart Cards. Unlike most hardware security modules, Intel IPT with PKI is designed to be managed as software but hardware resistant against tampering. The hardware based security is achieved by using the Intel® Management Engine (Intel® ME) to perform all cryptographic operations. This way, the keys are never exposed to software running on the computer's central processing unit (CPU). Furthermore, all certificates are tied to the platform on which they are created.

HP-Performance, Management and Security.
Banks and insurance companies feel attracted to companies that consistently meet their needs.

For **mobile professionals** in constant movement it is essential that the technology can suffer falls and knocks and still be available at any moment with great autonomy. They need fast connectivity and reliable performance to ensure the work is carried out correctly.

What they need: mobility, durability, connectivity.
In the case of **high executives**, a 'c-suite' offices calls for a 'c-suite' PC, designed for the style and performance of the executive class. Due to an overload of work, they need to have quick access to their data. They manage confidential information and need to be sure that all that information is safe.

What they need: security, performance and reliability.
In order to meet the requirements and expectations of mobility solutions and the required specifications of a biometric signature solution, HP has launched the **HP Elite Pad 1000 G2** and the **HP Elite X2 1011** series.

Figure 7: Tablet HP ElitePad 1000 G2 with Productivity Smart Jacket.

The **HP Elite Pad 1000 G2** has been designed for professionals who need mobility and to maximize productivity with the convenience of a tablet. This tablet uses a 4-core **Intel Atom** processor, 4GB memory and 64 or 128GB storage and is therefore able to work correctly with **Windows 8** and perform at the highest level with an extraordinary battery life.

These characteristics make it very interesting for professional environments. However, where it stands out is in the range of accessories to adapt it to different environments. There are "Jacket" adaptors that cover the tablet, protecting it against falls and extending its connections. Several models are already available:

- **Security Smart Jacket**, includes a Smart Card reader and the fingerprint to authenticate the user.
- **Productivity Smart Jacket**, includes Bluetooth keyboard.
- And finally, one designed for the needs of the **hospital and health sector**, and another that transforms the tablet into a **point of sale**.

Additionally, there is the possibility of adding a Stylus Atmel, which detects 256 levels of pressure and which, with the appropriate software, allows biometric signature recognition.

The **HP Elite X2 1011** is both a tablet and an ultrabook. Designed for business, this high-mobility unequalled-durability device is fully equipped with the renowned security and management capacity of HP. The equipment of the device also includes the powerful Windows 8, the 5th generation Intel Core M processor and a long-life double battery supplied for both the tablet and the keyboard.

It has the capacity to recognize biometric signatures through **Wacom** technology.

Figure 8: HP Elite X2 1011 G1.

	Elite Pad 1000 G2	Elite x2 1011 G1
TARGET	Mobile worker	Executive & Mobile worker
POSSITIONING	Tablet for enhanced productivity	Premium detachable with focus on mobility and design
PERFORMANCE	Permanent Support/ 24h	High Performance/ User experience
RELIABILITY	HP Total Test Process/Mil Spec tested	HP Total Test Process/Mil Spec tested
DOCKING SOLUTION	Expansion Smart Jacket / Bluetooth	Docking Wireless, Keyboard Base
BIOMETRIC SIGNATURE CAPACITY	Amtel Stylus Technology (Optional)	Wacom Technology
SECURITY	Smartcard and fingerprint scanner (Optional)	100% Smartcard and fingerprint scanner
BUILT	Aluminum	Aluminum

Figure 9: Comparative HP Pad 1000 G2 vs HP Elite x2 1011 G1.

HP Elite solutions include a wide range of security and management tools:

- **HP BIOSphere***, which is used to simplify the remote implementation and administration of the HP devices.
- **HP SureStart*** helps users recover their BIOS when damaged.
- **HP Touchpoint Manager*** helps staff in IT departments to manage devices remotely through the e-cloud.
- **HP Total Test Process*** tests the HP Elite products for 115,000 hours to confirm their resistance.
- **HP MIL-SPEC 810G*** tests to check if HP Elite products are capable of fulfilling the expectations of reliability.

Complementary technologies for Biometric Signature Solutions.

Currently there are between 20 and 320 applicable biometric technologies, each one with its own characteristics, which make them more suitable for one application or another. The combination of two or more biometric technologies in an integrated solution is a rapidly growing development, both technologically and commercially, as it provides more flexibility and accuracy.

The main characteristics of the most common biometric solutions are detailed below:

Fingerprint: the identification through fingerprints is widespread, having been used for dozens of years. The capturing device can be a desktop peripheral or a reader integrated within the mobile device.

Face recognition: this kind of recognition is based on the facial structure of the individual, registered by a camera by measuring distances and relations between points and creating a unique model of each person. The devices most frequently used are video cameras or the cameras integrated in the PC or tablet.

Iris recognition: by scanning the iris, a camera registers an image of the person's eye, which is a unique model. The "iris code" generates one of the most precise prints of all biometric technologies. The device used for the iris recognition is an infrared camera.

Voice recognition: the process of voice recognition depends on the characteristics of the physical structure of the individual vocal tract, as well as on the characteristics of behaviour. This recognition is carried out through a microphone or phone.

Hand recognition geometry: verification of the palm of the hand is easy, cheap, safe and has many applications in various economic fields. It is carried out with a scanner able to recognize the pattern of the lines on the palm of the hand.

Keyboard typing recognition: the typing dynamic is a branch of the biometry that studies the recognition of a user's typing pattern. This pattern is based on the speed and the pressure the individual exerts on the keys. The device used for this purpose is the keyboard itself.

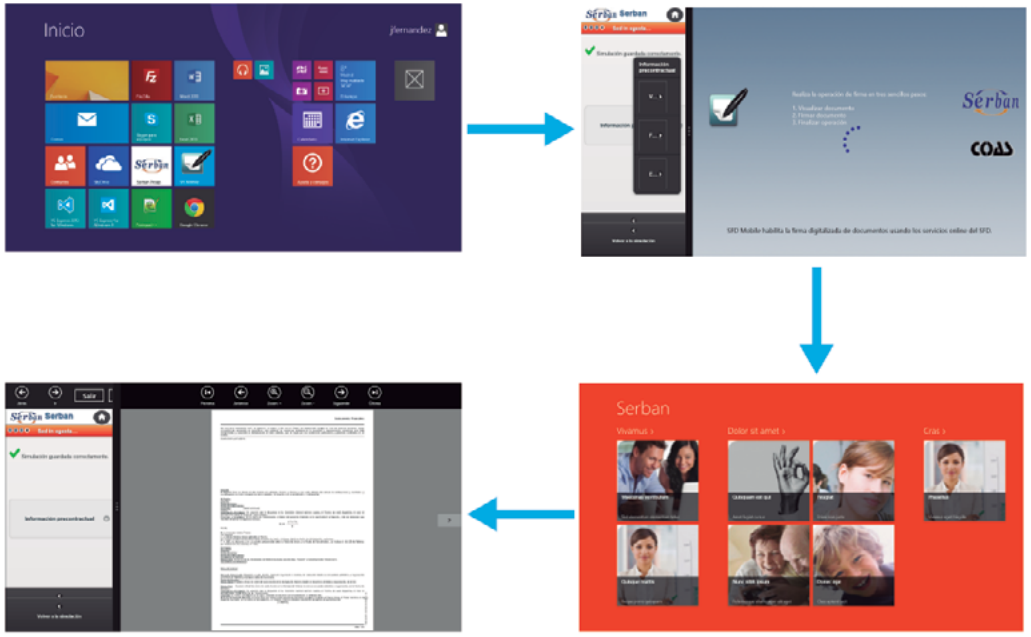
All these technologies combined are further enhanced by Intel IPT.

User perception of the Solution.
As most people are used to using their signatures when interacting with customers or providers, the Biometric Signature is considered less invasive than other biometric techniques.

The document does not leave the central server where it is stored; it is presented on the mobile device screen in PDF format with a space already prepared to be signed. Consequently, the user's feeling when signing on the mobile device is the same as when signing on paper, especially considering that the signature is filed in real time.

Both managers and customers can access the **BeSign** biometric signature application easily and quickly from the mobile device touchscreen and via the icons of Windows 8.1 operating system.

Once the application is working, the options **Visualize document, sign document** and finish operation appear:



With the selected document on the screen, the user has the possibility to zoom in using the buttons on the top of the page, or by sliding two fingers on the device's touchscreen. This tool makes it much easier to view the document.

By clicking on the "**Sign**" button at the bottom of the page, the user can see a window with the signers' names and the options **sign** or **omit**.

When the user selects the signer, the rectangle corresponding to the signing area grows bigger for more comfort. Once signed two buttons are presented: **Accept**, which sends the associated signature to the biometry server; and **Cancel**, which deletes the strokes to enable a new signature. After accepting the signature, a new **confirmation** is required in order to continue with the process.

Once the signature has been sent to the server, the user can explore the signed document and continue on to the following signer. The intervening parties that have already signed the document appear as disabled on the screen. This way the 'Finish' button is activated in order to proceed to the conclusion of the signing operation.

Factors to be considered in the design of the Platform types of integration.
Depending on the technological platform the entity currently has, and after a period of consultancy and analysis, there are some factors to take be taken into account when the decision to implement a Biometric Signature solution is going to be made:

Infrastructure currently deployed at the client's site: It is very important to know and understand the infrastructure the client is currently using so that the implementation of the solution is properly dimensioned and integrates without any compatibility problems (operating system, cloud environment, storage, communications, etc).

Volumetric study: based on the volume of the documentation managed by a company over a certain period of time, a volume analysis should be carried out in order to establish a dimensioning appropriate to the scope and infrastructure of the solution.

Stress Testing: a system stress test should be established for evaluation and dimensioning, depending on the number of tasks and mobile devices accessing the system at the same time.

Typology of the documentation: depending on the different types of documents managed by the financial entity (registration and cancellation applications, personal loans contracts, mortgage contracts, investments, etc), templates must be adapted and synchronized to ensure they are functioning correctly.

Study on the use of the MDM system (Mobile Device Management): with the purpose of implementing a system of centralized management of the mobile devices that are part of the solution.

Fixed Environment or Mobile Environment: depending on the working environment, the solution must be designed to work in an office, where only the implementation of fixed devices with accessories to capture biometric signatures will be taken into account; or in a mobile environment where, apart from the fixed office devices, the solution must provide tablets able to recognize biometric signatures. With the 2 in 1 devices both areas are covered, the fixed as well as the mobile office.

Mobile Devices: taking into account the conditions to which the devices will be subjected to, choosing the most appropriate solution is key. Battery life, capacity of biometric signature recognition, screen brightness, security, speed and communication systems are the most important determinants.

Use comfort: both the application and the mobile devices must be easy to handle. It is essential not to have any doubts about the use of the solution when dealing with a customer, as this can generate uncertainty when signing the document.

Compatibility Study: the **BeSign** Biometric Signature solution of **Serban Biometrics** is compatible with any type of cryptographic device that complies with the biometric recognition requirements. Any kind of document can be signed and configured for the different signature formats.

Standardization: the **BeSign** biometric signature solution is based on standard technology, that is, it is compatible with all web browsers, easy to use and integrate, configurable and parametrical to the client's needs.

Finally, security becomes a key aspect in a solution, which deals with a people's biometric data. It is necessary to remember that the security measures pointed out by the "Protection Of Personal Data Act" and its implementing regulation are not only requests for legal compliance, but also an example of good practices that can reduce and sometimes prevent potential incidents regarding users' privacy.

Applicability to other sectors with similar challenges.
The financial sector and the insurance companies are not the only industries susceptible to the introduction and use the biometric signature technology. There are many other sectors with similar challenges, where security in the identification of persons and optimization of resources make the proposed solution a fundamental asset.

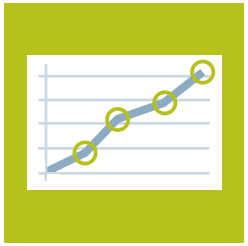
Health sector: what generates most paper in hospitals and health centres are informed consent documents. These are a legal obligation and by converting them into an electronic format these centres would benefit in terms of efficiency, cost reduction and regulatory compliance. The patient's or the closes relative's authorization to proceed with surgery, the doctor's signature after hospitalization to discharge the patient, the signature on a prescription or even a death certificate are all cases where the implementation of the biometric signature is especially important.

Public Administration: identification of persons who travel and must obtain a visa at customs, accessing public buildings or even recognition of signatures in public documents, applications, certification of documents, etc.

Real Estate Agencies: This solution is applicable to all those companies where the signing of documents is an essential part of their daily business. In any notarial or legal notice, public deeds, wills, assignments, sale or renting of property the acceptance and signing of documents is essential.

Industry and Commerce: applicable in the establishments, payments in cash, customer service, signing of contracts, logistics... In all these cases signing is required to confirm the reception of material, as well as acceptance of payment.

Legal: also applicable in electronic files, legal processes, complaints, lawsuits, etc. In courts there is a huge volume of documentation to be signed by lawyers, secretaries and citizens. Power of attorney, register of notifications and lawsuits, judgments and any other document that enters the court must be signed and registered as valid.



Using systems of recognition based on biometry on mobile devices brings great benefits for the organizations and entities that implement them. By allowing the generation of electronic documents at source, it is possible to disregard the physical format, which results in significant cost savings thanks to the elimination of paper, its manipulation, transport, storage and filing, among other things, apart from the time spent in finding and managing the documents once signed and filed.

The proposed solution described here focuses on helping companies from the financial and insurance sector to optimize their processes by means of the signing of documents on devices that allow absolute mobility. The key benefits for the business the proposed solution can offer are:

Document Control: Banks, savings banks and insurance entities manage millions of documents every day. The management and manipulation of these documents generates a huge volume of work, physical space requirements, logistics and time investment. With the **BeSign** solution for biometric signature recognition errors, losses, storage and damage of documents is avoided, as the use of paper formats is no longer necessary. The documents in electronic format are under control, in a safe environment and accessible from anywhere at any time.

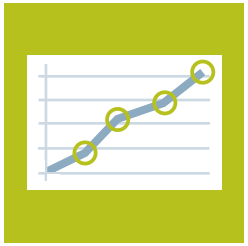
Cost reduction and optimization of productivity: biometric signature enables greater agility and security in the contracting process, since a document can be signed by different people in different places at different times. It also means losses and errors are reduced, with a consequent saving in costs. Thus, taking as an example a medium-size financial entity with Average Total Assets of 85,000M€, 1,300 offices and around 55 million operations a year, the potential reduction in costs would be:

- Direct costs: elimination of paper would mean a saving of **1,500,000 €**.
- Operative Efficiency: reduction of **45,000 hours.**
- Savings in indirect costs: **1,940,000 €.**

Improvement/Reengineering of processes: the constant evolution of technology and the need to implement projects that meet both the internal needs of each company and their customers' expectations are the main challenges that those responsible for IT departments face every day. With the automation of processes offered by the **BeSign** solution, all the tasks regarding signatures, verification, encryption and filing can be carried out in the minimum time and always under control.

Technological innovation image: With cutting edge technology and latest mobile devices, companies adopting the biometric signature solution offer a modern and innovative image to customers, while transforming its work processes.

Fraud Prevention: With the ability to obtain customer's authentication at the moment of signing, encrypting



the signature, and storing securely with the document, this solution reduces the chance of fraud.

"Green Office": the elimination of paper and the use of printers (ink or toner) from the signing processes help reduce the environmental impact. A medium size financial organization has the potential of saving 110 million sheets of paper with electronic solution, which represent saving 14,903 trees a year[4].

Increased Security: the documents to sign are never lodged in the mobile device; they are lodged in a central server. The mobile device only shows an 'image' of the original and the signed document.

For more information:

To learn more about **BeSign de Serban Biometrics**:
http://www.serban.es/en/solutions/biometrics-digitalized-signature

To learn more about **Intel Processors**:
www.intel.com/content/www/us/en/processors/atom/atom-processor.html?_ga=1.2986047.1216291211.1440865489
http://www.intel.com/content/www/us/en/processors/core/core-m-processors.html

To learn more about **Hewlett Packard Tablets**:
www.hp.com/country/us/en/uc/welcome.html

To learn more about **Microsoft Windows**:
www.microsoft.com/en-us/windows

[1] Source European Central Bank (Europa Press 12/08/2013) www.europapress.es/economia/finanzas-00340/noticia-banca-cerro-1963-oficinas-espana-2012-357-total-eurozona-20130812120618.html.
[2,3 & 4] Source Serban Biometrics Studies.

IIntel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at www.intel.com.Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.

No computer system can be absolutely secure.

Cost reduction scenarios described are intended as examples of how a given Intel-based product, in the specified circumstances and configurations, may affect future costs and provide cost savings. Circumstances will vary. Intel does not guarantee any costs or cost reduction.

*Other names and brands may be claimed as the property of others.