



Signed, sealed, delivered...
digitally

A new platform for confidential, legally binding
digital communications

Information kit



Content

03

Signed, sealed,
delivered... digitally

04

Who is
Woobe for?

05

How does
Woobe work?

09

Woobe as legal proof
("virtual legality")

11

Confidentiality,
security and
data privacy

15

Woobe pricing

16

About Woobe

17

Frequently asked
questions

19

Woobe and specific
client segments
(examples of uses)

Signed, sealed, delivered...digitally

Up until now, no technology has been able to fully guarantee user identity. In the eyes of the law, passwords, PINs, most electronic signatures and even static fingerprint IDs have all failed to prove without reasonable doubt that a person using a system is who they say they are. That matters when your content is confidential, business-critical or intended to be legally binding.

Now, thanks to Woobe's unique biometric system, information can be signed, sealed and delivered digitally over the web in complete confidence. Users can be anywhere worldwide, providing they have access to a computer and a Woobe ID device.

Woobe guarantees the legal value of digital exchanges by reliably identifying content authors, senders, receivers and other mandated parties at every critical step through dynamic fingerprint matching. User consent or agreement, another essential aspect, is built into the process.

Woobe also ensures complete confidentiality by encrypting documents and unlocking them only for authorized individuals. Every transaction is authenticated and timestamped, providing accurate confirmation to users and, if necessary, the law.

Designed to provide technology as irrevocable legal proof or "virtual legality," Woobe guarantees data privacy by eliminating the need to store personal data on a central database. It is the only solution that meets the strictest international guidelines for electronic communications and data privacy set out by the United Nations, the European Union and OECD and translated into law, including European Directive 1999/93/EC and 910/2014 on the use of e-signatures in electronic contracts. On this basis, Woobe has already been endorsed by the French data protection authority, CNIL.

Woobe's easy-to-use system is compatible with Microsoft Windows and soon all major operating systems, including mobile. With a Woobe personal data card and portable ID device (a combined card reader and dynamic fingerprint scanner), users can access the system in seconds through their preferred digital environment.

Developed from a concept designed by a former magistrate, Woobe is being used by a growing number of auditors, lawyers and other professionals who require fail-safe communications in a legally binding environment.

Who is Woobe for?

Woobe is suitable for any kind of organization or individual wishing to establish a binding contract or communicate digitally with the highest levels of confidentiality, security and data privacy.

Applications include

- ▶ Providing a financial guarantee or letter of credit
- ▶ Signing a price quote or issuing a purchasing order
- ▶ Giving instructions to suppliers
- ▶ Announcing a general assembly to members of a board
- ▶ Providing proof of sending or receipt of an important document
- ▶ Sharing highly sensitive corporate information
- ▶ Ensuring secure exchanges when working remotely
- ▶ Signing or agreeing to changes in a contract
- ▶ Any other action requiring complete confidentiality, traceability and legal validity

Woobe is used by a growing number of auditors, lawyers and other professionals who require fail-safe communications in a legally binding environment. It is also attracting interest from organizations as a way to manage the risks associated with data protection.

“ Woobe has solved the uncertainty of digital transactions, without mentioning significant productivity gains ”

Philippe de Lacvivier , Auditor.

Data security, data losses and cybercrime: a growing expense for companies

Worldwide spending on information security will reach \$76.9 billion in 2015, according to a forecast by IT research consultancy Gartner, Inc. with the growing use of mobile, cloud and social technologies creating new vulnerabilities.

Data security regulation is likely to tighten in Western Europe and Asia-Pacific, driving further spending on data security. Examples of relevant regulation include:

- ▶ European Directive 1999/93/EC and 910/2014
- ▶ The Australian Privacy Act (1988)
- ▶ Personal data protection laws in Singapore and Malaysia (2013)
- ▶ (Non-binding) guidelines on personal data protection in China (2013)

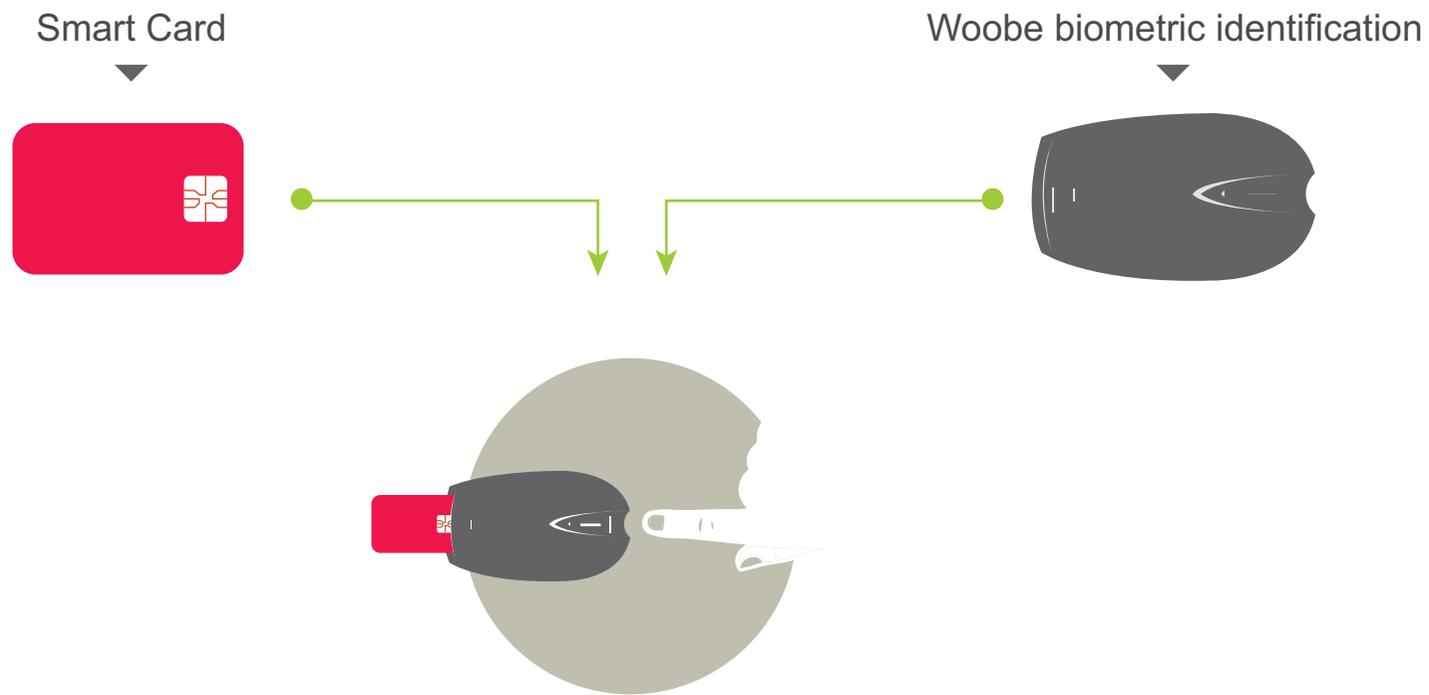
The annual cost of security breaches and data losses amounts to an average of \$860,000 and \$586,000 respectively per company, according to a global survey carried out by data storage specialist EMC Corporation in 2013:

- ▶ 61% of all respondents' companies had suffered at least one of the following incidents: data loss (29%), security breach (23%) or unplanned downtime (37%).
- ▶ The top four consequences were: loss of employee productivity (45%), loss of revenue (39%), loss of customer confidence/loyalty (32%) and loss of incremental business opportunity (27%).
- ▶ Globally, the cost of data losses reaches an estimated \$754 billion (€660 billion)

Cybercrime is estimated to cost the global economy more than \$400 billion annually and growing, according to the Center for Strategic and International Studies (2014) and security software company McAfee. At particular risk is the financial industry, since its assets are the easiest to monetize.

How does Woobe work?

Woobe is easy to set up and quick to access from users' normal desktop (and soon, mobile) environment.



The user swipes his or her finger across the Woobe reader to generate a unique signature linked to a document

System requirements



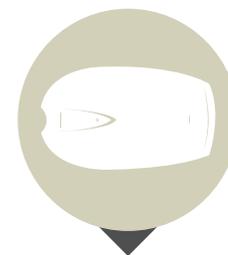
+



+



+



A computer

Woobe client software

Personal Woobe fingerprint data card

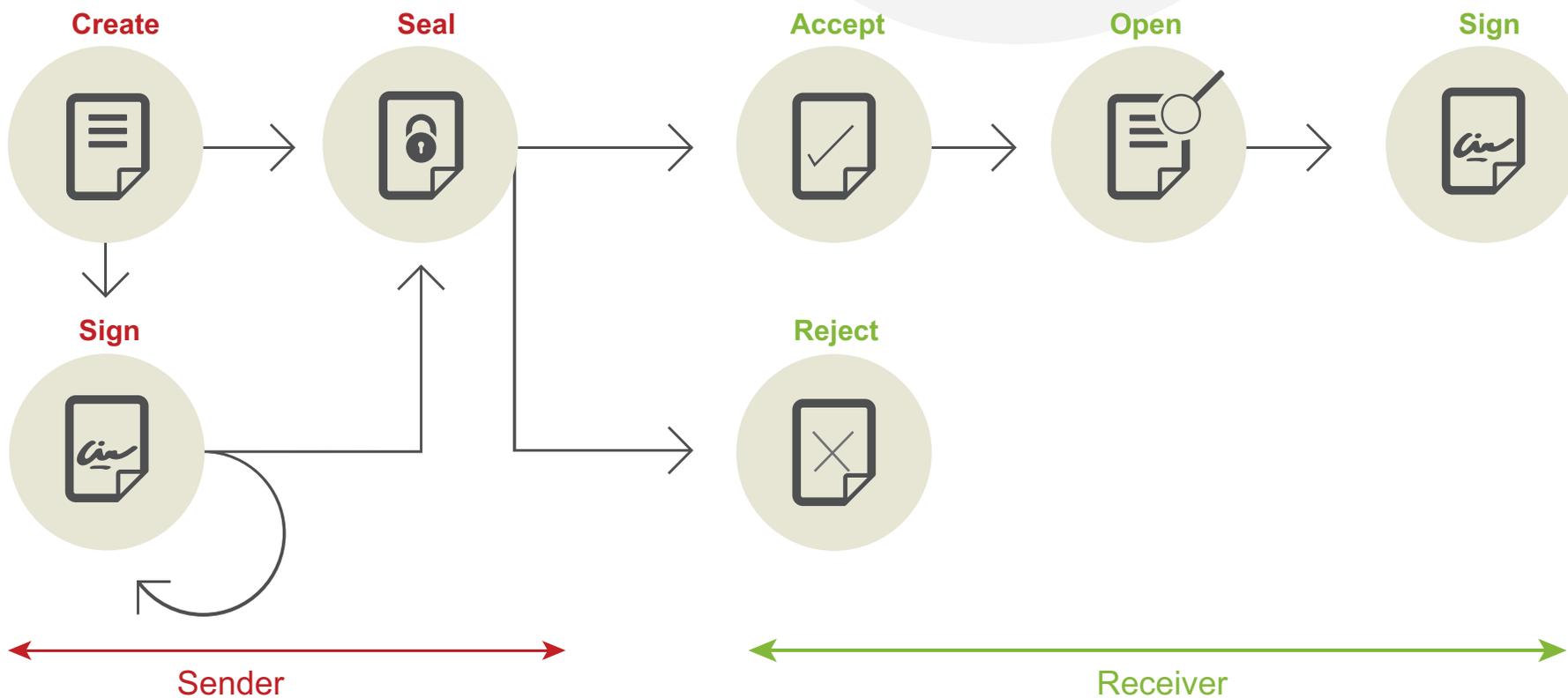
Woobe ID reader

(Microsoft Windows 7 or higher and soon all major operating systems, including Apple OS X)

Woobe personal data cards and ID readers are available upon request, usually within five days of requesting a Woobe account. The client software can be downloaded from woobe.fr

Step-by-step

Woobe's unique exchange server ensures confidentiality, security and data privacy from end to end. Documents are accessible to authorized signatories only and every main action (creation, acceptance, refusal, signature, etc.) is tracked. No personal data is stored on a central database or server.



Woobe enables users to act on content and follow critical developments (create, sign, seal, accept, open, follow up, consult and archive).



1. Identification

Users log in by inserting their personal ID card into the Woobe ID reader (a combined card reader and dynamic fingerprint scanner) and swiping a finger across the scanner. If the fingerprint and swipe movement match the card data, the user is identified and can enter the Woobe system. Given that the probability of two identical fingerprints is 1 in 10^{24} and the system also requires a match with the user's swipe movement, this particular two-factor identification provides unbeatable levels of security (a failure rate of 1 in 18 million).



2. Authorization

Once inside the Woobe interface, users can select the documents they wish to access. Woobe only decrypts content when the user has proved with his card and finger that he is an owner of the document. (Authors designate specific recipients, and general parameters can be set when installing Woobe.)



3. Action: sign, seal, deliver...and more

Users can create, seal, accept or refuse, open, sign and archive content in complete confidence, thanks to Woobe encryption. Documents are authored from Word, ERP, and other office applications, and then converted to PDF/A (ISO 19005 standard) by Woobe client software so as to ensure their long term visual integrity. Structured data can still be attached to enable automated data processing by enterprise gateways. Users may sign documents as a natural person (themselves) or a legal person (e.g., in their official capacity as director, lawyer, bailiff, accountant, etc.). Further, content can be signed by multiple signatories, as defined by the document owner.

At any time, users can copy Woobe documents onto a memory stick, shared drive or even cloud storage and forward them to a mandated colleague for signature in complete confidence. All versions of the document are synchronized by an original process that solves a paradox: one legally unique original document will ever exist although physical copies can be multiplied at will.



4. Tracking/legal proof (Optional)

Every transaction is authenticated and timestamped, providing accurate confirmation to users and, if necessary, the law. This tracking information is stored within each document and can also be verified with a QR code reader.

Documents can only be opened by authorized, identified users.

The Woobe reader guarantees document confidentiality.

Users can request a QR code of timestamped information.

Woobe is the only technology solution to enable legally binding digital communications worldwide. For electronic exchanges to serve as **legal proof**, several requirements need to be met:

- ▶ **Irrevocable proof of identity.** Users must be identified with complete certainty at every critical stage (document creation, signing, sending, etc.). This is where Woobe's biometric sign-in comes in. No other system (PIN, passcode, etc.) can provide the same level of legal certainty.
- ▶ **Irrevocable proof of consent.** Users must be able to consciously accept or reject content for consideration. Content is not considered delivered until the user actively seeks it out in their Woobe mailbox and accepts it. Again, proof of user identity is critical here.
- ▶ **Proof of agreement.** A commitment must be considered definitive and irreversible, as confirmed by a “signature” or other form of inalterable proof. The Woobe system does this by requiring users to provide fresh identification (using the Woobe card and fingerprint device) whenever clicking on the «sign» button.
- ▶ **Integrity, one original document.** Anyone signing an agreement must be certain that the original content has not been tampered with. Woobe tracks and timestamps on each document the delivery, first opening, and signatures.
- ▶ **Supranationality.** Woobe complies with most stringent international rules on data privacy, identity, signatures, and trusted third parties: OECD guidelines, EU regulations (EC)45/2001, COM 2012/011 (GDPR), directive 1999/93/CE, UE 910/20014 (eIDAS), United Nations trade law UNCITRAL 1996, 1998, 2001.
- ▶ **Third-party proof.** In a legal dispute, the accused and defendant cannot be their own witnesses. With Woobe, every critical action (document creation, signing, sending, etc.) is linked to a user identity and timestamped, leaving a certified trail. Woobe therefore acts as a witness or third-party certifier.

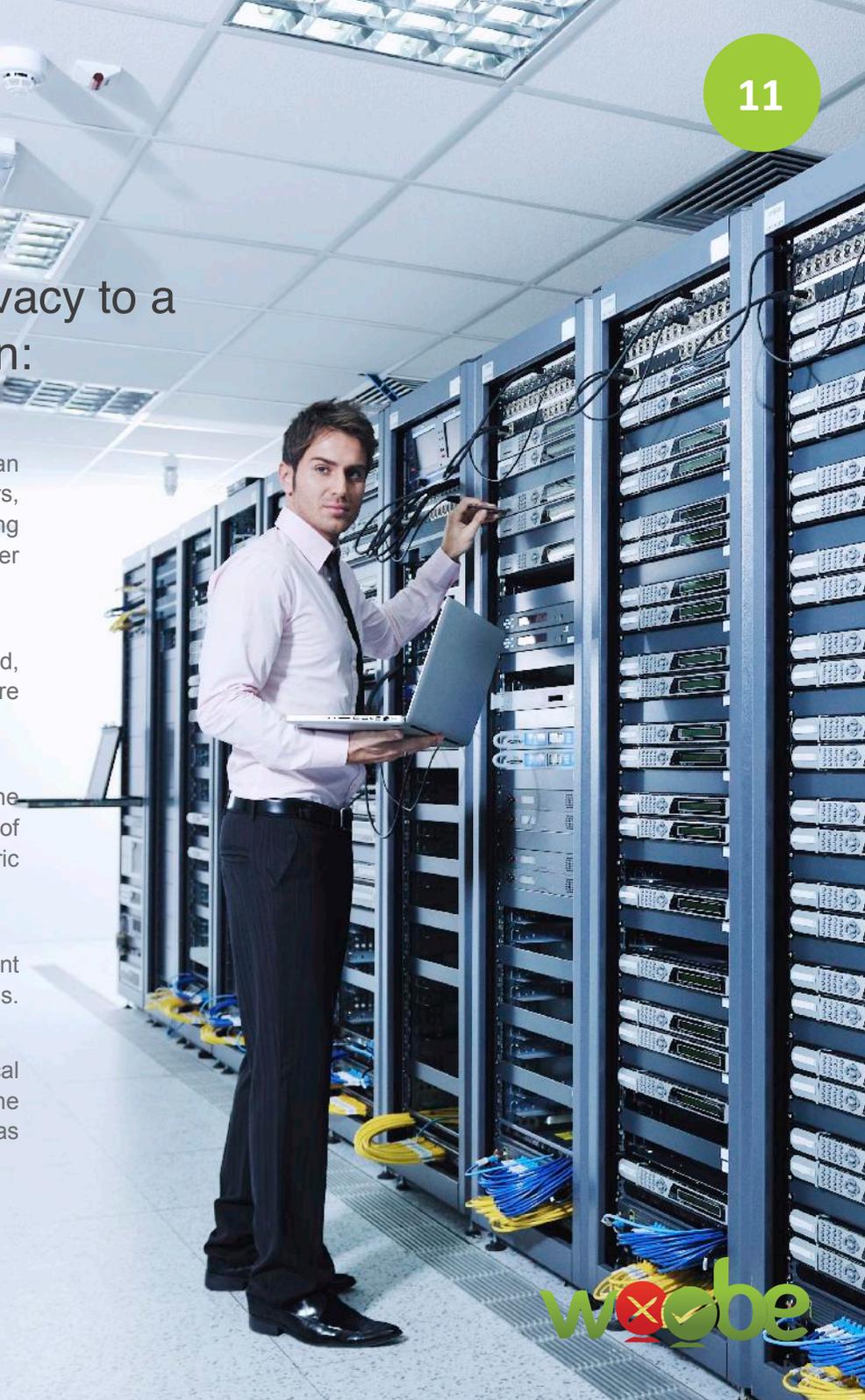
Woobe vs. electronic signatures in the eyes of international law

Legal requirement	Woobe based on dynamic biometric identification and encryption software	 Existing e-signature solutions based on public key infrastructure (PKI) technology and encryption software
Irrevocable proof of identity	 The user’s identity cannot be stolen: every action in the Woobe system requires biometric identification.	 Keys can be copied and PIN codes lent or spied. The e-signature provides an indication of the user’s identity but not irrevocable proof.
Irrevocable proof of signature	 The user’s irrevocable identity is required to sign a document (or carry out any other action: sign, seal, accept, open, ...)	 Since the user’s identity is not proven irrevocably, the signature cannot be considered definitive.
Ability to act in an official capacity (e.g. in a specified role on behalf of an organization)	 Woobe enables users to sign in and act as a private person or legal representative. They can also mandate individuals to act on their behalf or authorize them to access specific documents and carry out specific actions (sign, seal, accept, open, ...)	 Alternative authentication systems cannot guarantee the user’s identity or the capacity in which he or she wishes to act.
Irrevocable proof of consent	 Users are informed of new content in their Woobe mailbox and must actively identify themselves to accept documents (if they wish to).	 The fact that documents are sent or opened does not imply consent by either party (sender or receiver).
Third-party proof	 The Woobe system timestamps all actions carried out by each user within every document. If necessary, this very precise reporting data can be used as legal proof.	 Other systems only guarantee the technical integrity of documents. Standards like PDF signatures allow editing and provide no delivery trail. When providers have an audit trail, it is centralized and thus violates personal data protection rules.
Data privacy	 Personal data can only be accessed by the owner, thanks to Woobe’s match-on-card biometric technology. No personal data is ever stored on a central database or server.	 Existing centralized systems build third party proof in centralized trails and therefore lack privacy.

Confidentiality, security and data privacy

Woobe raises data confidentiality, security and privacy to a new level by combining several layers of protection:

- ▶ **At the user level,** by storing personal identification (fingerprint) data on cards rather than a central database. Woobe “match-on-card” technology ensures complete data privacy for users, since their biometric information never leaves the card and can only be activated with matching dynamic fingerprint data (from the user swiping a finger over the Woobe scanner in his or her usual way).
- ▶ **At the document level,** by encrypting content and restricting access to authorized, identified users through dynamic fingerprint matching, which is one of the most secure authentication solutions available (see below).
- ▶ **At the system level,** by separating the document storage and working functions. The Woobe browser, which is integrated into the user’s operating system, simply presents a list of encrypted documents. Authorized users must identify themselves using the Woobe biometric process in order to access and act on documents (open, accept, refuse, sign, send, etc.).
- ▶ **At the network level,** by storing documents in the cloud on highly secure, redundant Woobe servers. No content can be accessed without decryption through the biometric ID process.
- ▶ **At the legal level,** by identifying users and timestamping their actions at every critical step. No changes to documents can be made without the relevant users’ knowledge, and the agreement process for any contractual content is fully documented in a way that can be used as legal proof.



Dynamic fingerprint matching: a highly secure three-factor identification process

Unlike other solutions, Woobe's identification process offers an almost-zero rate of error (1 in 18 million) by combining several unique elements:



The user's fingerprint. The probability of two user's fingerprints being identical is around 1 in 10^{24} and the Woobe system will not work with forged static fingerprints (see below).



The user's swipe action. In addition to correct fingerprint data, Woobe identification requires a match with the user's typical swipe movement, where the swipe speed curve also makes a difference.



The user's personal Woobe ID card. Each fresh identification attempt must match the fingerprint and swipe data contained in the user's personal Woobe card. This data remains in the card and is never transferred to any central database.

Woobe security: a new military-grade approach

Woobe has invented a completely new system to guarantee that only document owners can ever open a document using their smartcard and fingerprint identification. Consequently, documents can be copied and stored on different media without compromising security because security is intrinsically bound to each individual document. Even if the encryption code could be broken on one Woobe document, the hacking process would have to start from scratch on the next...

Security at the user's fingertips, literally

Woobe uses matching-on-card biometric technology with a sweeping thermal sensor embedded into the smartcard reader. This means that a user can only be authenticated after swiping a live finger across the reader in his or her usual way. No data enters the user's computer, and unlike passcodes, there is nothing visible that can be stolen by onlookers or malware. Woobe's smartcard has been designed to meet military-grade security (EAL5+ or Evaluation Assurance Level 5 of 7, an international standard). Woobe's encryption and identification system is so robust that it overrides the need for security at the network and storage levels. Here, it is more important to ensure redundancy.

No central files = absolute data privacy

Personal data privacy is not just a concern but a requirement. The Woobe system ensures absolute privacy in terms of personal data, document content and reporting, by encrypting data using a variety of algorithms (RSA, AES-128 and RIPEMD-160). All personal data is stored on the card and can only be accessed by the only person it relates to: no one else can read or change the information on the card.

Thanks to Woobe's "full match-in-card" technology and unique messaging system, users are protected from cyber spying and out of reach of "GAFA" (Google, Apple, Facebook, Amazon) and the other major private companies that have access to massive amounts of personal data. The system becomes a virtual safe, without windows or doors for prying eyes.

In a future release, Woobe plans to flood the system with an avalanche of fake number records to further protect the real data.

Legal authentication if necessary

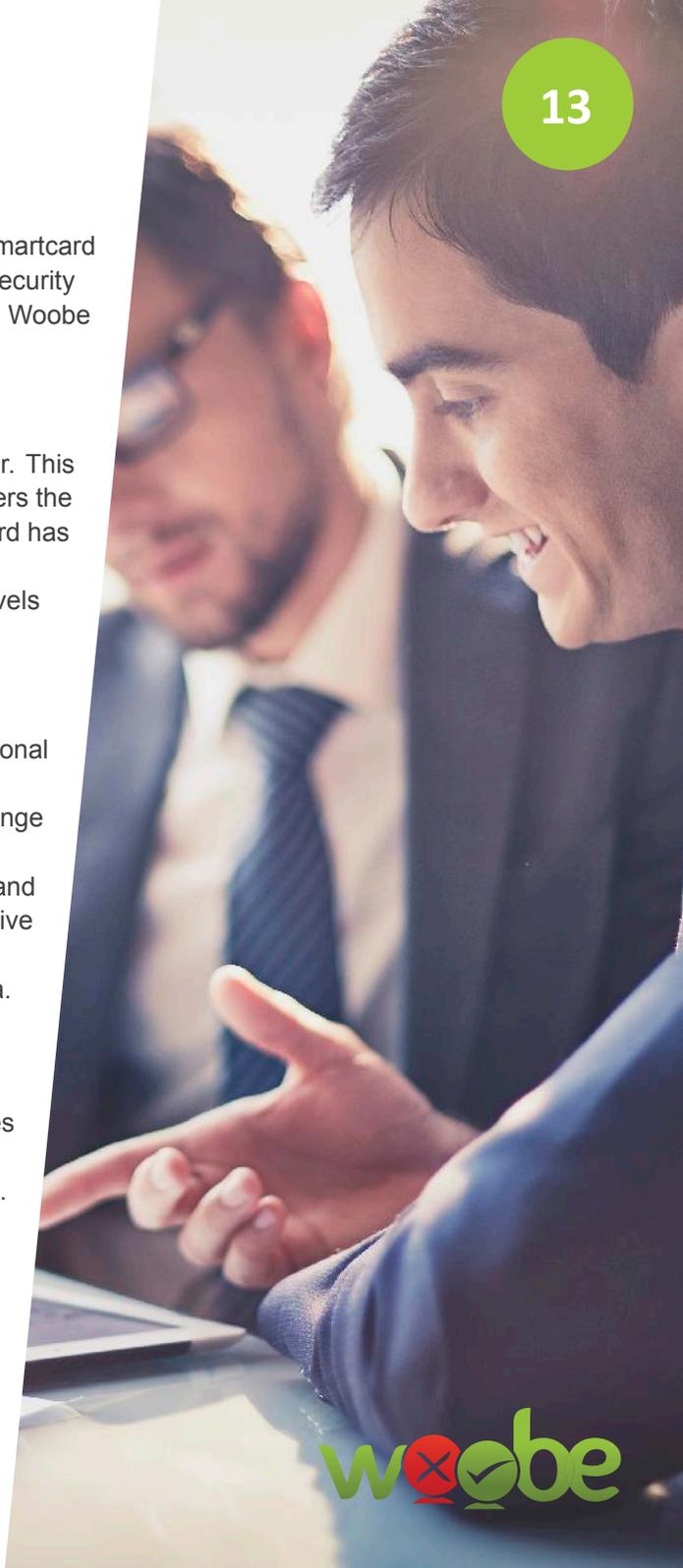
Woobe can act as a trusted third party to legally vouch for the authenticity of documents and all related signatures and identities without opening them, using a technique similar to zero-knowledge cryptography.

Further, users can mandate forensic investigators and/or judges to access selected documents in the event of legal proceedings. If necessary, Woobe can also identify users, who may then be ordered by courts to provide access.

Unique, new and proven

The Woobe system is so different that existing certifications do not appear relevant (e.g., for data center security) when the security resides in the encryption and identification processes.

The company therefore asked two renowned cryptography experts, Professor Jean-Jacques Quisquater and François Koeune of UCL Crypto Group to audit the system. Their conclusion? Woobe works!



Woobe features

Sign, seal and deliver content in complete confidence with Woobe...

Features and functions

▶ **Sign-on as a natural or legal person**

Woobe enables users to sign on as a natural person or legal person (director, lawyer, accountant etc. representing an organization).

▶ **Multiple signatories and contractors**

Users can invite specific colleagues to review and sign a document before sealing it. They may also invite multiple recipients to sign a document, and set a timeframe.

▶ **Mandated users**

Users can delegate others to act on their behalf, using their own ID.

▶ **Notification**

Users can be notified of pending documents on any device.

▶ **Right to accept or refuse**

Users cannot be forced to accept any documents they do not want to receive.

▶ **Accurate tracking without a central database**

Each document contains complete tracking information (when each recipient has accepted/refused, opened or signed a document, etc.).

▶ **Flexible workflows**

Woobe documents can be copied onto memory sticks, hard drives or cloud storage and forwarded to colleagues in complete confidence, since only authorized users can access the content. All versions of documents are automatically synchronized.

▶ **Full data protection and confidentiality**

Only mandated owners (document creators, signatories, recipients, etc.) can open documents, based on dynamic biometric identification. Security is guaranteed by Woobe's unique identification and encryption system.

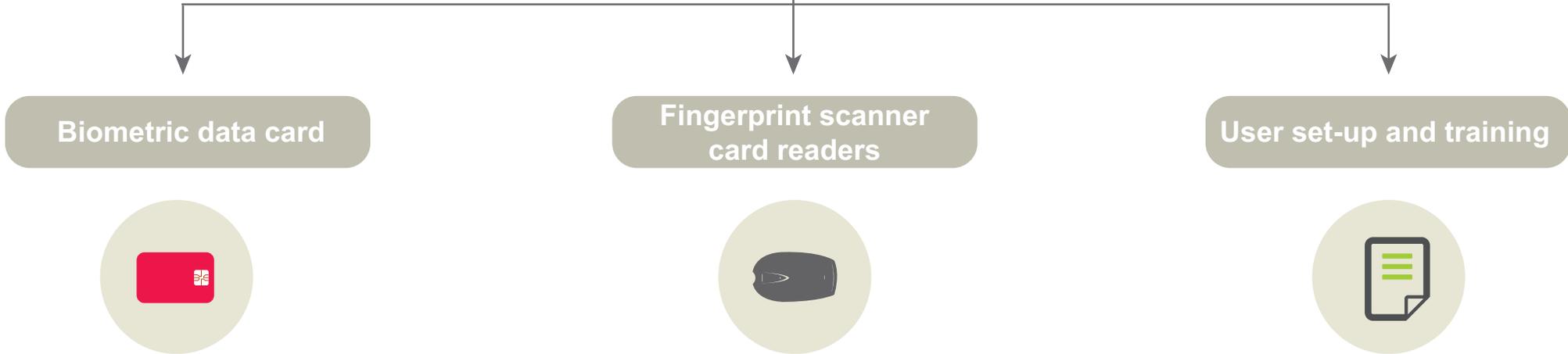
▶ **Legal compliance**

Woobe meets the strictest international regulation regarding data privacy and legally binding communications.

Woobe charges each sender **1€** per document sent per recipient, with discounts for large off-peak volumes.

Customized set-up packages are available on request, including:

- ▶ Each user's personal biometric data card
- ▶ Woobe dynamic fingerprint scanner/card readers
- ▶ User set-up and training



Our company

Woobe enables information to be signed, sealed and delivered electronically in complete confidence thanks to a unique system based on biometric authentication and digital encryption. It is the only technology solution to guarantee the legal value of digital exchanges by reliably identifying individual users at every critical step.

Woobe was founded in 2010 by former magistrate Philippe Morel and two business partners, Alain Llorens and Bernard Hauzeur. The company is owned by the three founding partners and a board of investors. Woobe is based in Paris, France.

Founders



Philippe Morel
Founder and CEO
Former magistrate



Bernard Hauzeur
Founder and CTO



Alain Llorens
Founder and COO

Investors and board members



Michel Poss
Project Director Compliance
& Risk Management



Olivier Bougé
Business
development manager



Vincent Lebunetel
CEO at Boost.rs
board member of Welcome
City Lab and Tech'4'Team

The Woobe name

Woobe is pronounced “woo-be”, similar to “who be?” and the Chinese “wǒ bì” (我必), meaning “me for sure.”
The aim was to put the accent on identity, which is critical to Woobe’s two key benefits: legality and confidentiality.



→ Can anyone use Woobe?

Yes, Woobe is suitable for any organization or person wishing to establish a binding contract or communicate digitally with the highest levels of confidentiality and security. Woobe enables users to sign in their official capacity (e.g., as a sales director rather than a private individual) and to limit their legal responsibility to a specified amount (e.g., up to €100,000).

→ Who are Woobe's clients?

In its initial phase, Woobe is already being used by auditors, lawyers and bailiffs in France and abroad. The company is also in talks with a number of international institutions to set up the system organization-wide.

→ How long does it take to open a Woobe account and get started?

Woobe is currently available to major organizations on a case-by-case basis after a feasibility study. In France, set-up takes five working days on average.

→ What are the system requirements for Woobe?

Woobe is currently compatible with Microsoft Windows 7 & 8, and will soon be available on all major operating systems, including Mac OS X and mobile.

→ Can I use Woobe on my mobile?

Woobe is currently available for desktop/laptop use only. A mobile version is under development.

→ Can the Woobe interface be customized to my organization?

Yes, Woobe can be customized to any organization and new features are being developed with clients to meet the specifications of their industries.

→ How much does Woobe cost?

Woobe costs €1 per document sent, with discounts possible for large volumes sent off-peak.

→ Do recipients pay a charge?

No, there is no fee for receiving a document, but all users must be connected to the Woobe system. A per-document charge is charged to the sender.

→ Can I send Woobe documents to users who are not connected to the Woobe system?

Yes. However, the recipient will not be able to oppose any claims as he is not a Woobe user.

→ Is there a limit to how many documents I can send or store?

The only limit is the storage capacity of your IT equipment.

➔ What file formats can Woobe handle?

The Woobe client software uses PDF/A, the only standard file format able to guarantee that all document users, in particular signatories, see the exact same content. (PDF is no longer proprietary Adobe software but an ISO 19005 standard.) Woobe can convert all common formats (Word, OpenOffice, Excel, Access, etc.) and professional applications (CAD/CAM, ERP, CRM, etc.) into PDF/A.

By design, PDF/A (“A” for Archive) cannot be edited and can therefore serve as proof of a document’s integrity. The PDF/A-3 variant enables the original Office format (and other structured data) to be attached to the native PDF/A so that recipients can reuse the data, but without the visual integrity guaranteed by the original PDF/A file.

➔ What reporting tools does Woobe offer?

Every user can access a detailed index of all his or her exchanges, which can be sorted and viewed through filters. In addition, each document contains a timestamp of every critical action (when content was created, updated, signed, etc. and by which user) to serve as legal proof if necessary.

The way Woobe is designed to protect confidentiality means that no one – not even Woobe administrators – can access a detailed breakdown of user traffic. The Woobe server simply counts the number of message recipients and total volume sent for billing purposes.

➔ What technical support do you provide? Do you have a hotline?

In addition to detailed information on the Woobe website, we offer telephone support during extended office hours (7 a.m. to 7 p.m., Monday to Saturday).

➔ How is Woobe more secure than other solutions on the market?

The Woobe system is built around a unique form of dynamic biometric sign-in, which is one of the most secure methods of authentication on the market, combined with data encryption. Users can rest assured their data remains confidential no matter which device they use. There are no security risks because every Woobe document is encrypted and can only be opened with the user’s matching card and dynamic fingerprint data.

➔ Can Woobe be used as legal proof in any country?

Yes, absolutely. Woobe guarantees the legal value of digital exchanges by reliably identifying content authors, senders, receivers and other parties at every critical step through dynamic fingerprint matching. User consent or agreement, another essential aspect, is built into the process, while data privacy is ensured by storing no personal data on any central database. Woobe complies with the strictest international laws, such as the European Union’s Regulation (EC) No. 45/2001 on data privacy.

➔ What are the risks involved in using Woobe?

Woobe takes the risk out of digital communications by making them highly secure and tamper-proof, and providing a documented trace. Only authorized, identified users can access content intended for them.

Client segment	Potential uses (examples)		
	External:		Internal:
Financial service providers	<ul style="list-style-type: none"> ▶ Creating contracts online ▶ Offering loans and confidential, contractual personalized deals ▶ Statements ▶ Bills of exchange ▶ Debt recovery 	<ul style="list-style-type: none"> ▶ Factoring ▶ Financial orders ▶ Guarantees 	<ul style="list-style-type: none"> ▶ Managing delegation of authority ▶ Circulating and processing applications and approval processes
Auditors and legal communities	<ul style="list-style-type: none"> ▶ Instant registered e-mail ▶ Certified signatures ▶ Certified dates ▶ Confidentiality agreements ▶ Liaison between lawyers, courts and other legal experts (bailiffs, solicitors...) 		<ul style="list-style-type: none"> ▶ ▶
Marketplaces and e-commerce players	<ul style="list-style-type: none"> ▶ Calls for tender, price quotes, specifications, orders, delivery instructions, notices and invoices ▶ Guarantees ▶ Insurance ▶ Copyright and brand protection ▶ Increased confidentiality for competing users 	<ul style="list-style-type: none"> ▶ Confidential personalized offers, pricing, terms and conditions, etc. ▶ Creating contracts online 	<ul style="list-style-type: none"> ▶ Securely tracing and archiving information
Small-medium enterprises	<p>External & Internal</p> <ul style="list-style-type: none"> ▶ Exchanging any kind of information confidentially, securely and in a legally binding manner. 		



For more details, please contact:

Philippe Morel
Founder and CEO

Phone: +33 (0)6 88 78 40 29
pmorel@woobe.fr
www.woobe.fr

