

neBULA**SUITE**[®]

Providing banks and financial institutions with legally compliant digital signatures based on qualified digital certificates



vintegris**TECH**


Executive Summary

Digitalization of services means more opportunities for banks to develop their economic activity fully and at worldwide level. Financial institutions are currently in a moment of transition from a traditional model to a digital one, but are already well-aware of the benefits that this new paradigm provides them, such as the reduction in paperwork-related costs, more flexibility for online transactions, and an increment in the number of online financial operations done—in summary, an increase in business activity.

Digital signatures are part of this digital landscape. Banks are starting to increasingly use them to facilitate transactions and save costs, since they provide legal compliance and help avoid identity theft and fraud, thus increasing trust, which is key for this kind of organizations. This paper examines the relevance of digital signatures for banks and financial institutions, specially regarding:

- Digital certificates and digital signatures
- The difference between electronic and digital signatures
- The benefits of the paperless organization
- The importance of legal compliance (eIDAS)

This document will help organizations understand the complexity of digital signatures, by providing them with accurate information about the many benefits that their adoption will bring to them.





Introduction

Banks and financial services rely on trust. Among the current needs that this sector is experiencing in its shift towards complete digitalization, there are three that are particularly pressing, and that directly affect trust: legal compliance, reputation, and the security of the customers' personal data.

Nowadays, with the digitalization of their services, it's not enough for banks to simply have information about customers, employees, services, or electronic devices that interact in a system. They must be able to securely identify them and ensure that only authorized ones can access bank applications and data. Once trust is established this way, banks and other institutions must protect it.

But there are other obligations to fulfil, such as adhering to a rapidly changing compliance landscape, meeting high customer expectations, and efficiently managing digital transactions and services, which generate massive amounts of data.

Digital certificates to provide digital identities

Digital certificates help keep trust intact through encryption. A digital certificate is a key used to grant a digital identity to a person or electronic device in a system. It can be compared to a passport, in the sense that it has a unique and non-transferable number associated with a user, issued with guarantees by a recognized certification authority (CA). This CA verifies the identity of each user through a process called

vetting, thus eliminating the possibility of identity fraud and forgery. Regarding financial institutions' customers, these certificates will allow them to get identified when doing multiple business transactions with banks. Digital certificates are used for robust authentication (thus providing convenient services with secure access) and for digital signatures (also known as electronic signatures or e-signatures).





Legally binding digital signatures and banking business

Digital signatures are based on digital certificates. They guarantee that the signatory is who he claims to be, through an algorithm. This way, the signed document gets protected against identity theft.

The digital signature market is growing at a fast rate. Business Wire mentions some of the major growth factors that could help drive the adoption of digital signatures in Europe: "secure & reliable transactions, authenticating the identity of the user over the digital network, and the new release of regulations for electronic signatures by the European Electronic Messaging".¹

Toward the paperless bank

Digital signatures are being widely adopted for many reasons:

- They are more difficult to forge than paper signatures.
- They are more secure than paper signatures, due to the encryption technology they use.
- They are more economical, since they reduce paperwork-related costs (printing, transport, storage, and destruction of documents), and help keep documents organized.

According to Derek Brink, co-founder of the PKI Forum, the cost of manual document processing is high.

Each paper document is copied 9-11 times at a cost of approximately \$18 (€15), and filed at a cost of \$20 (€17). In addition, there are costs of storage, printing and distribution of the document.²

The paperless conception of the banking organization also implies a greater consideration for the environment, since it contributes to the reduction of carbon emissions, which are in part to blame for the greenhouse effect.

There is no doubt that the general adoption of the digital signature will contribute to a paperless future for banks, or at least to a considerable reduction of the amounts of paper they use.

Are electronic and digital signatures the same?

With the gradual disappearance of paper and the slow adoption of the digital signature, we are often confused by the terminology used. On a daily basis, it is common to see that the terms electronic and digital signature are indistinctly used, as if both were synonymous and interchangeable. However, we must bear in mind that all digital signatures are electronic, but that not all electronic signatures are digital:

- Electronic signature: is the one that is used to sign a document. An example can be the handwritten signature on a touch screen.
- Digital signature: is the one that, through an algorithm that encrypts the document, guarantees that the signatory is really who he claims to be. This way, it protects the document against identity theft and fraud.

It should be noted that both of them are accepted and used in many companies and organizations, but the digital signature offers a higher level of security; therefore, many banks and financial entities are incorporating it among their technologies.

eIDAS and the importance of legally binding digital signatures for banks

Legal compliance is important when choosing a solution for digital signatures. In the European Union, eIDAS (Regulation EU N°910/2014 on electronic identification and trust services for electronic transactions in the internal market) was implemented in 2016, to avoid lack of mutual recognition of electronic signatures between member states. This regulation makes it easier to do business, sign agreements and close transactions within the EU.

eIDAS establishes three types of digital signature: simple, advanced and qualified. The qualified signature fulfills several requirements, including allowing the identification of the signer and being linked to the signed data —it also has the legal equivalence of the so-called “wet signature”, is recognized within the EU and is based in qualified certificates, which means greater protection of the data.

Having a legally binding digital signature with full legal guarantees is more than convenient for financial institutions. It's fundamental.

What are the benefits of legally-compliant digital signatures?

A digital signature based on a qualified digital certificate issued by a Certification Authority (CA) protects the document with encryption and gives greater security to the information contained therein. In the same way, customers and employees of banks are able to sign documents digitally anywhere, either from their workplace or on the go, while complying with eIDAS.

In addition, employees can approve and sign documents from their computers, smartphones or tablets, to accelerate sales, approval cycles, legal reviews and international transactions with entities such as the European Central Bank, SWIFT, ICO, and the CNMV. And on the other hand, external customers can digitally sign contracts for greater convenience and time savings allowing:

- The transformation of the geographical dispersion of customers and employees into business opportunities through the use of digital signatures, eliminating bottlenecks in productivity processes.
- Faster signing processes with public agencies or other financial institutions.
- Easier transactions for clients when their signature is required (policies, loan agreements or credit card applications).

¹ <https://www.businesswire.com/news/home/20170306005908/en/2.65-Billion-Digital-Signature-Market-2017-Solution>

² http://www.oasis-pki.org/pdfs/Financial_Return_on_Investment.pdf

About vintegrisTECH

vintegrisTECH manufactures innovative systems and applications for digital certificate management, digital signatures, and robust authentication. Its flagship product is **nebulaSUITE**, a comprehensive solution for guaranteeing digital identity, authentication, and secure access, as well as its own Certification Authority (CA).

nebulaSUITE is the only solution in the market that provides banks and financial institutions with the full infrastructure for qualified digital certificates (issuing and management) and legally binding digital signatures through cloud-based services —all protected by robust authentication.

vintegrisTECH's clients include leading banks, insurance, health, retail, government, and public-sector organizations.

For more information

If you are interested in getting more information about **nebulaSUITE**, contact us at info@vintegris.tech or visit www.vintegris.tech



vintegrisTECH

Barcelona
Madrid
London
San Francisco

vintegris.tech
info@vintegris.tech
[linkedin.com/company/vintegristech](https://www.linkedin.com/company/vintegristech)
twitter.com/vintegrisTECH
+34 934 329 098



eIDAS
compliant