Arthur D Little

Telecommunications, Information,
Media & Electronics

Digital Signatures

Paving the Way to a Digital Europe

Content

Authors:

Nicolai Schaettgen
Principal
TIME, Austria
schaettgen.nicolai@adlittle.com

Didier Levy
Director
TIME, France
levy.didier@adlittle.com

Julien Duvaud-Schelnast
Manager
TIME, France
duvaud-schelnast.julien@adlittle.com

Sorana Socol
Business Analyst
TIME, Austria
socol.sorana@adlittle.com

Introduction

Digital signature solutions are quickly replacing paper-based signatures and have the potential to dominate signature-related processes. The primary benefits of this technology include increased efficiency, lower costs and increased customer satisfaction.

Processes that still require a handwritten signature slow down turnaround time, increase complexity in terms of archiving, and also raise environmental issues with regards to paper usage. Companies are therefore increasingly adopting digital signature solutions to address those challenges.

The financial services industry is the pioneer in the adoption and development of digital signature solutions, and we expect other industries, such as telecommunication, commerce, utilities, notaries and healthcare, to follow soon as the benefits of this new technology, namely increased efficiency, lower costs and increased customer satisfaction, are not restricted to any industry. While offering clear advantages, digital signature solutions still need to overcome some challenges, such as the need to adapt existing systems and processes to the new technology, concern about acceptance by business partners and the perceived high cost.

The European Union is currently finalizing regulation, which will increase the legal value of advanced electronic signatures and remote electronic signing services by offering the possibility to generate a qualified digital signature using a remote signing system. The regulation is expected to be enacted in early July 2014. This development is expected to serve as an example for other markets on how to approach digital signatures from a regulatory standpoint.

This report is based on Arthur D. Little's survey of 50 market experts in Europe, as well as comprehensive secondary market research. In this report, we provide an overview of the digital signature technology, its current and potential market, as well as the benefits and challenges it brings. We also present examples of practical applications of digital signature solutions.

Digital Signatures

Authenticity and Integrity of Data Provides a High Level of Security

Digital signature solutions are quickly replacing paper-based signatures and have the potential to dominate signature-related processes. The primary benefits of this technology include increased efficiency, lower costs and increased customer satisfaction. Digital signatures need to be clearly distinguished from ordinary authentication processes. While authentication is only used to verify the identities of end-users, digital signatures also ensure the integrity of data. A combination of these two security factors is critical for many business transactions, especially those involving sensitive and confidential data.

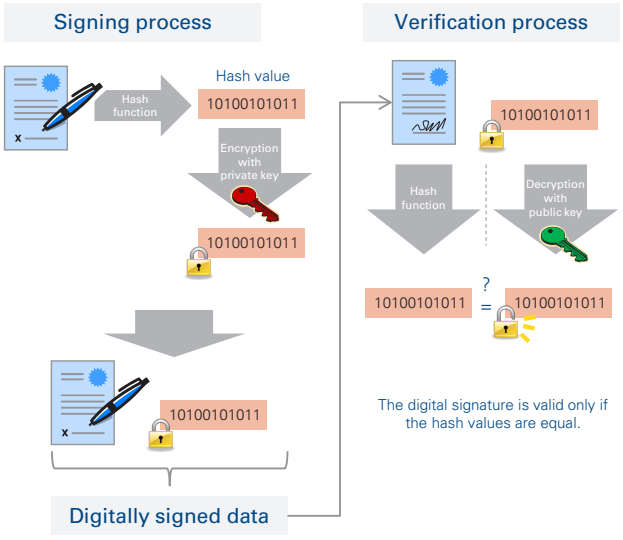
Digital signatures are a sub-category of electronic signatures. While an electronic signature can be any kind of data attached to a document, such as a written name below an email, a digital signature is based on a mathematical process of protecting the document. There are two major types of digital signatures, differentiable only by how securely the authentication has been processed:

- **Qualified digital signature (QES)** is a signature that is created with a secure signature-creation device, other than the device where the document is actually signed, which provides very high security;
- **Advanced digital signature (AES)** is a digital signature where the signature could be created on the same device where the document is signed, which is somewhat less secure than QES

A digital signature involves three processes: the signing process, the authentication process and the process of ensuring the integrity of data. The process of creating a digital signature is the same, whether internally or externally managed.

- The *signing process* starts by providing an end-user with a document that needs to be signed. In order to be sure that the correct person signs the contract, the end-user's identity is verified by multiple factor authentication, such as a PIN, password and sequence-based token codes. Once the identity is verified, the signer receives a certificate proving his identity and providing him with a pair of keys: a private key (known only to the signer) and a public key (known to the public). These keys are necessary to sign a document and to verify the identity of the signer. Once the certificate is issued, a unique mathematical code is created out of the document. This mathematical code is then encrypted with the private key (signing) and can only be decrypted with the corresponding public key (verification of signature). The document, together with the encrypted mathematical code, is then sent to the recipient.
- In order to *ensure authenticity,* the recipient with access to the public key can decrypt the mathematical code and is therefore able to ensure authenticity. The public key works for decryption only if the document was signed with the corresponding private key already confirming the identity of the signer.
- The *integrity of data* is ensured through a mathematical code, which is visible to the receiver after the decryption. To verify that the document has not been changed by any unauthorized person, the receiver calculates his own mathematical code out of the document. If both codes match, the integrity of the data is ensured; if the document had been changed in transition, the receiver's calculation would give a different code.

Figure 1: The Digital Signature signing and verification processes



Source: Arthur D. Little

Figure 1 illustrates the signing and verification process on the basis of the RSA (Rivest, Shamir and Adleman) cryptosystem technology, which is the most widely used encryption technology.

The encryption process described above provides the foundation for the high security and the legal validity of this technology. The mathematical encryption combined with a high quality certificate ensures the integrity and authenticity of the digital signature. The resulting advanced digital signature is covered under EU law and therefore legally valid.

Any process not encompassing these security measures are not regarded as secure or legally valid. Remote and face-to-face transactions should therefore be based on the above procedure of securing data. For example, a handwritten digital signature on a signature pad without a digital signature created is not legally valid in court decisions, based on the precedent legal case from June 2012 in Germany[1]. Other commonly used techniques encompass the recognition of biometric data, such as the speed or pressure of the signature, in order to authenticate the signatory. This technology is certainly more secure than a simple handwritten signature on a signature pad, but it is not covered by EU law or most national laws and provides therefore no legal validity.

There are two major ways to offer digital signature solutions to end-users: an externally managed process and an internally managed process. Although both have advantages and disadvantages, based on analysis of market trends, Arthur D. Little believes that the externally managed process will be the solution of the future.

Externally managed process (external Public-Key-Infrastructure or PKI)

During the externally managed process, an external company provides the certificates needed for the digital signature. The third party is responsible for providing one-time certificates to employees and / or customers of the company after they have been authenticated. With a fully externally managed process, companies do not need to invest in set-up and maintenance, which results in a lower overall cost of implementation.

Preferably, the external service provider should offer a **full cloud solution**, the primary advantage of which is that the certificates are not stored on any SSCD (Secure Signature Creation Device or token), but in the cloud and can therefore be used on any device. Furthermore, no specific Software as a Service (SaaS) has to be installed, increasing the level of trust and convenience for the customer. Studies have shown that customers who are asked to install software when digitally signing are more likely to cancel the process. For customers, the strongest incentive is convenience. Digital signatures are a much easier way to sign for a document compared to plugging an e-ID card into a PC and even to the traditional handwritten signature. The cloud enables companies also to offer multi-channel signatures (e.g. one signature from home, the other from mobile phone). As mobile signing from a tablet or smart phone becomes more popular, a cloud-managed service will be the preferred technology. This was also confirmed in the interviews Arthur D. Little conducted, in which one market player responded, *"Why should we ask customers to carry always a token or smart-card reader with them?"*

It is important to mention here that this type of concept makes the most sense if the third party is a **trusted** one, such as on the EU trusted list. This will not only raise the overall level of trust, but the certificates provided by a trusted third party are recognized virtually worldwide, which means that the root certificate, a certificate that is verified as trusted, is already installed in most browsers and operating systems and no error message will appear as with the internally managed process.

With cloud solutions, there is also the possibility to perform the signature with an SSCD or a smart card. Here the cloud can be used to securely archive the digitally signed documents.

Internally managed process (internal PKI)

The certificates needed for the digital signature are established and provided internally by the company offering these solutions to employees or customers directly. Certificates are not one-time certificates, but can be reused, as they are stored on specific badges, such as a token, smart cards, etc.

The concept requires an infrastructure that securely manages identities and corresponding certificates. The process of implementing a PKI involves an investment into hardware, software, and training for employees, and is therefore rather applicable for larger corporations with the corresponding knowledge and resources. A major drawback of the internal PKI concept is that the certificates are in most cases not trusted by browsers and operating systems, unless the company is on the EU trusted list.

Depending on the resources available and the level of trust and control required, each company has to weigh which solution suits it best. However, there are already indications that solutions where additional external devices are needed to create digital signatures will not be popular with the general public. 15 European countries deployed electronic identity cards (eID)

1 http://www.justiz.bayern.de/gericht/olg/m/presse/archiv/2012/03561/

containing credentials for online authentication, with a majority also offering an optional digital signature function. To be able to make use of this digital signature function, a card reader for the eID needs to be bought, further complicating this concept.

The potential of this solution could, however, be improved with NFC (Near Field Communication) technology enabling the usage of the digital signature with eIDs without a card reader, such as with an NFC smart phone. Although the ability to sign using a smart phone would guarantee a higher level of mobility, it is expected that full cloud solutions not requiring any card or card reader will dominate the future market for digital signatures, as the level of convenience provided will be the decisive factor in the choice of solution.

Benefits Include Decreased Costs and Greater Efficiency

Digital signatures can be implemented in a variety of areas as companies can use digital signatures for their internal processes or communication with business partners and customers. Governments are also an important category of customers for this technology, as they are increasingly required to implement leaner and cost-minimizing processes.

Many companies and governments have already realized the potential of this technology. A fully digital process of signing and sending documents decreases work hours and reduces cost in paper and transport. Arthur D. Little's survey and further analysis confirmed that the immediate adoption of the technology has the potential to create a sustainable competitive advantage independent of the industry in which a company operates.

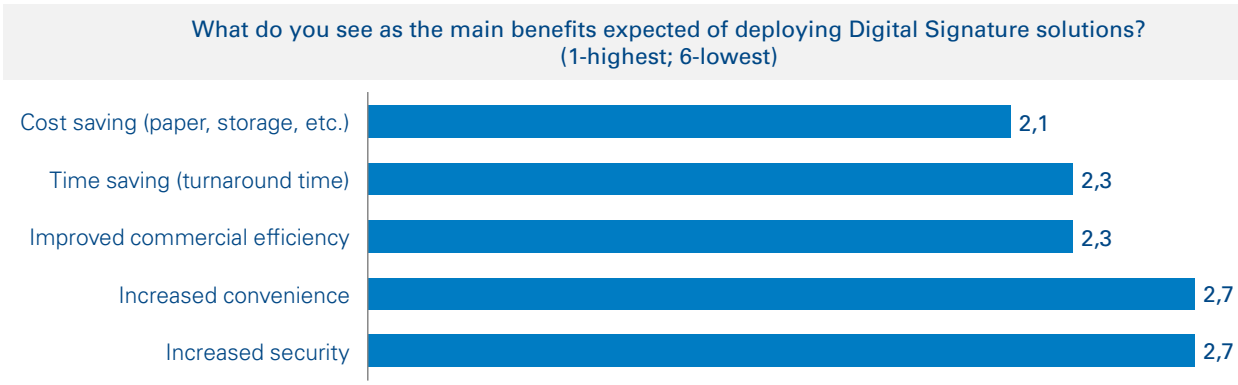
According to the results of Arthur D. Little's survey, the main argument for adopting the technology is to improve efficiency, leading to the reduction of costs, and to increase to the speed of the overall business. The use of digital signatures decreases costs by reducing processing costs, such as scanning, recording, archiving, printing and mailing, and reduces resource expense (less process cycle time results in lower personnel expenses). Business processes are also made more efficient by increasing the overall agility of enterprises (reduced process cycles, speed of closing business) and through the real time tracking and coordination of business.

Besides efficiency considerations, adopting digital signature solutions portray a progressive image of both the user and the provider of such technologies. Also digital signature solutions have the potential to increase customer convenience. For example, a bank can offer its customers multi-channel solutions to sign a loan agreement.

Although industry experts taking part in the survey did not regard increased security as a major benefit of the technology, digital signatures provide a higher level of security than traditional methods of sending documents, when implemented appropriately with cryptographic procedures with qualified certificates:

- The integrity of data can be ensured as counterfeiting is virtually impossible, while a paper document can be modified after being signed by an unauthorized person,
- The probability of losing a digital copy is much lower compared to paper-based documents,
- All types of data, such as photos or audio files, can be digitally signed, which protects the copyright of these materials,
- A timestamp can be attached to the digital signature, ensuring that the document was signed on a specific date.

Figure 2: The major benefits of Digital Signatures



Note: All numbers represent average values

Several Challenges Still Need to be Overcome

Despite the potential of the technology, the implementation of digital signature solutions also brings along challenges. A majority of companies have systems and processes designed around traditional methods of contractual communication. From an employee's desk to the archiving of signed documents, the *adaption of existing applications or systems* was regarded as a major issue in the interviews. Companies and institutions interested in adopting the technology are therefore highly dependent on trusted, easy-to-implement and convenient solutions that do not increase the complexity of workflows. Suppliers able to offer this important mixture of characteristics will likely have substantial competitive advantage in the market for digital signature.

Furthermore, there is still an issue with the *acceptance of business partners/customers*. From the survey, however, it was clear that this acceptance is strongly dependent on the solutions offered to customers, meaning that a broad range of use cases guaranteeing ease of usage will raise the acceptance of natural and business partners.

There was also the impression among respondents that implementing digital signature solutions will incur a *high cost of investment*. This argument is applicable in the short-term, but reduced costs offset the cost of investment generally in a very short time. The cost of a particular solution depends on the type of implementation. Cloud solutions result in lower implementation cost. The overall cost, however, depends on the solution's pricing model and on the frequency of usage.

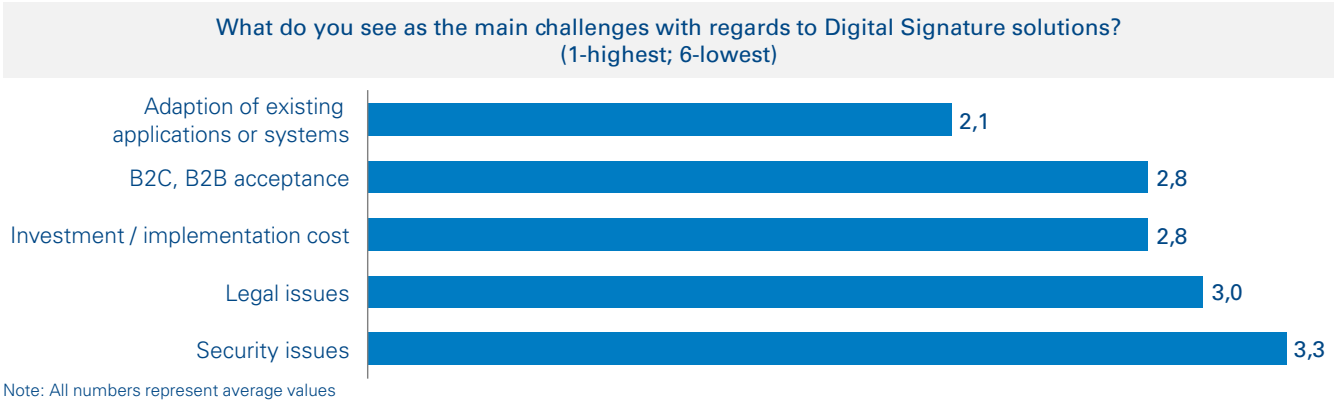
Certified email could present a risk to digital signatures

Certified email is a service that is also aiming to ensure a secure transfer of data between sender and recipient by enabling emails to be encrypted by the sender and decrypted by the receiver. In order to do so, the sender and the receiver need to have a certified email account with a certified email provider and software that is able to encrypt and decrypt emails. If authenticity of the sender plays an important role in the transaction at hand, the certified email can also be digitally signed (with a qualified digital signature).

A major security issue with certified email is that it is not based on an end-to-end encryption process, meaning that every email that was encrypted by the sender is decrypted by both certified email providers (email could be read or modified), representing a security issue that could be utilized by unauthorized parties. There is a possibility to enable end-to-end encryption, but only with additional encryption software.

Compared to classic digital signature solutions, email has security and convenience disadvantages as the standard model is not based on end-to-end encryption and because both the sender and the receiver must have a certified email account.

Figure 3: The primary challenges of Digital Signatures



Note: All numbers represent average values

New Legislation will Further Promote the Use of E-signatures

European legislation is predominantly based on Directive 1999/93/EC, which stipulates common obligations for certification service providers and common rules on liability and cooperative mechanisms in order to secure trans-border recognition of signatures and certificates throughout the European Community. The Directive addresses three forms of digital signatures: simple, advanced and qualified digital signature.

A new EU Regulation on electronic identification and trust services for electronic transactions in the internal market is expected to be implemented in 2014, in order to consolidate the use of digital identification and signatures throughout the European Union. Key cornerstones of new EU regulation include the removal of existing barriers to delivering a comprehensive cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions, as well as the potential to enable cloud signatures to achieve the highest level of security. Full cloud-based signatures will be able to be qualified once some final requirements are met.

The industry expert interviews conducted by Arthur D. Little confirmed the general impression that while the law is clearly defined, it is not yet transparent to the general public, creating challenges to the potential of the technology.

The Digital Signature Market is Highly Fragmented and Dynamic

To create a digital signature, it is necessary to have a secure environment, where the digital certificates needed to perform the digital signature are managed (issued, potentially stored, and utilized). This environment is called Public-Key-Infrastructure (PKI) and can either be locally managed in-house by the service issuer or can be externally managed by a cloud solution provider and accessed over the internet. In both cases, the service issuer, such as a bank, is offering the service to the end-user; either the token or other device where the certificate is stored is handed over to the end-user or the end-user is forced by the bank to sign via the cloud.

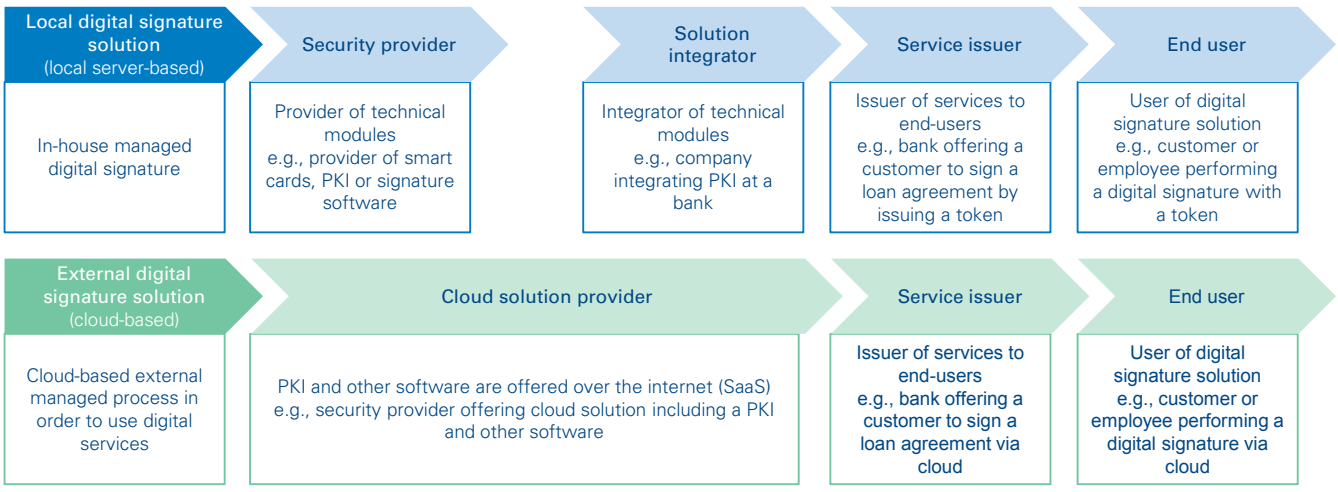
The parties involved in the implementation and application phases of digital signature solutions can be seen in full detail in the graph below.

The digital signature market in Europe is currently small, highly fragmented and dynamic. There are new players with new technologies, established players that focus only on the signature market and players from other industries that are trying to diversify. There are both European players, such as Opentrust and D-Trust, and American players trying to enter the European market, such as Adobe Echosign, ARX CoSign or DocuSign, which has already offices in the UK since three years. In order to facilitate their market entry in Europe, some of the US players have partnered with local players; Opentrust was selected by DocuSign as their European partner to jointly create a new digital signature solution, coupling EU legal compliancy and ease of use.

In order to highlight the complexity of the market and to give a comprehensive overview of the main actors, typologies have been identified and characterized using a bottom-up investigative approach. Fifteen main suppliers of digital signature solutions active on the European market have been assessed based on the chosen typologies.

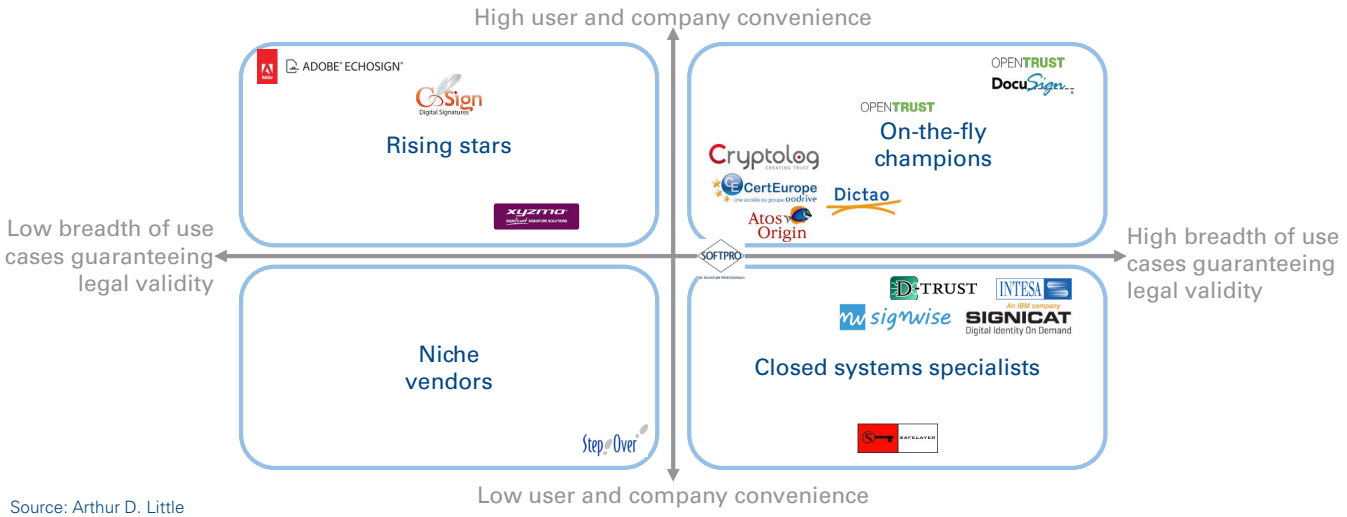
- **User and company convenience:** High user convenience means that the customer is able to process signatures from any computer, tablet or smart phone, no external devices (hardware token/ e-ID card) are needed and there is no need to install any software (SaaS). This high degree of convenience means that no internal PKI is needed, archiving (Evidence Management) is outsourced and there is no need to install any software (SaaS).
- **Breadth of use cases guaranteeing legal validity:** High breadth of use cases guaranteeing legal validity (supported by QES, or at least AES, based on qualified certificate), means the digital signature solutions offered to the customer enable many use cases supported by a certified supplier having the status of trusted third party.

Figure 4: The Digital Signature value chain



Source: Arthur D. Little

Figure 5: The Digital Signature market



Source: Arthur D. Little

Based on the defined dimensions we have identified four main typologies of suppliers:

- On-the-fly champions
- Closed systems specialists
- Niche vendors
- Rising stars

On-the-fly champions are suppliers offering highly convenient solutions for customers, such as financial services companies, banks, or other highly regulated industries, which by the nature of their work require lots of references and certifications to guarantee legal validity of digital signature. In a market where customer-friendly solutions (SaaS) are the key to success, on-the-fly champions are the most adaptable to customer needs and also have the highest legal validity of provided solutions. The clear leader among on-the-fly champions in Europe in both B2C and B2B is the French supplier, Opentrust, the inventor of offline and cloud signatures (cloud system certified ETSI TS 102 042, ETSI TS 102 023 and TüvIT). Positioned as an online notary (or trusted party) and having jurisprudence in its favor, Opentrust offers legally valid digital signature solutions with a high user and company convenience.

Closed systems specialists vendors offer non-cloud based solutions for medium and large companies with many customer interactions and a broad range of internal processes requiring the use of digital signature and who prefer an internal management of the digital signature solutions. Companies already having internal PKI systems and already using badges with certificates inside can reuse these certificates, however they need to manage the PKI system and the solution is strongly dependent of the operating systems and web browsers, which all evolve quite often. The Spanish player, SafeLayer, has an established presence on the European market especially as a provider of digital signature solutions for financial institutions and public administrations, which demand many legally valid use cases as well as solutions based on their own server, rather than cloud based, due to the high level of confidential data.

Niche vendors are suppliers offering internal solutions for smaller customers, not requiring many use cases or end user interactions. The solutions are not compatible with multi-channel / multi-device strategy, making the user experience less rich and interactive, however offering the advantage of internal management of the solution. The German player, StepOver, is a niche vendor providing both digital signature software, but also hardware components; there are 100,000 StepOver signature pads already in use. StepOver is the strong partner for smaller companies, preferring an internal management of their digital signature solutions.

Rising stars are small suppliers offering cloud-based, convenient solutions, but with a limited amount of use cases with no EU legal value, but they have the potential to become the next on-the-fly-champions, but they still have a long way to go in order to get certified (ETSI TS 101, 102 etc.), to get on the EU trusted list of verifiable certification authorities and to build a customer base. For example, the US-based digital signature provider, ARX CoSign, is still a small player on the European market. Offering user-convenient solutions, but with no EU legal value, CoSign needs further certifications in order to increase the legal validity of its products and thus its European customer base.

Use Cases Provide Insight into the Practical Application of Digital Signatures

Digital signatures can be applied in various workflows almost in every economic sector. Use cases embrace any kind of communication where a declaration of intent combined with authentication of the parties involved is needed or required by law. Beyond eID services, which according to secondary research have not yet been very successful due to the low usability of the overall solution, the real market belongs to cloud-based digital signatures due to the convenience of the solution; the customers can view the contract, tax return, import or export duties, etc. on any device - whether PC, tablet or phone - get sms for authentication and then sign with no need for any special hardware or software.

For the purposes of this report, we have used the following segmentation for digital signatures:

- Business-to-Business (B2B)
- Business-to-Customer (B2C)
- Government.

The use cases further distinguish between remote and face-to-face transactions.

- **Remote:** the signatory is signing the document without a physical presence of a representative of the service-offering company (e.g. bank); authentication is also done by a remote method (e.g. one time password, sms, etc.)
- **Face-to-face:** the signatory is signing the document with the physical presence of a representative of the service-offering company; this representative also authenticates the signatory (e.g. against a passport or ID document).

Common use cases in B2B	
Remote	Face-to-face
■ Internal management of documents ■ Supplier contract management ■ Customer contract management ■ Human resources contract management	■ Contract signing through roaming sales (e.g. insurance, corporate finance)

From the interviews conducted, current project requests and additional research Arthur D. Little recognizes a steep increase in the number of companies that are already transforming into "digital companies" or planning to do so.

Furthermore, it is observed that the acceptance of the technology is high in the B2B segment, as technologically advanced business partners are seen as role models.

Common use cases in B2C	
Remote	Face-to-face
■ Online subscriptions ■ SEPA SDD mandate management ■ Account creations	■ Contract signing on tablets in branches ■ Contract signing on tablets by retailers and distributors (e.g. loans, insurance)

The applied use cases in B2C depend very much on the legal validity and the overall customer acceptance of such technologies, which varies among different markets. Industries that are generally pioneers in offering these solutions to end-users are the delivery, banking and the insurance industry.

Common use cases in Government	
Remote and Face-to-face	
■ Online subscriptions ■ SEPA SDD mandate management ■ Account creations	■ Contract signing on tablets in branches ■ Contract signing on tablets by retailers and distributors (e.g. loans, insurance)

Governments are generally the main drivers for the cross-industry diffusion of the technology in Europe. Pressure to decrease costs is forcing many governments to think about making their processes leaner, while also guaranteeing security for sensitive commercial and personal data. Many governments in Europe offer or even oblige companies or citizens to communicate with them in a digital way.

Credit Agricole Consumer Finance Case Study[2]

The following case study on Credit Agricole Consumer Finance was prepared by Arthur D. Little, in collaboration with Credit Agricole's digital signature supplier, Opentrust, a leading provider of on-the-fly digital signature solutions in Europe in both B2B and B2C.

Company overview	■ Crédit Agricole Consumer Finance is a major consumer credit provider in France and in Europe ■ Products: Financial products and services (direct sales, point-of-sale financing, e-commerce, partnerships) ■ Operating in 22 countries
Main drivers for deployment	■ Customers expected modernization of workflows and products ■ Reduce cost
Concept of digital solution	■ Operating in 22 countries
Areas of application	■ Face-to-face transactions (B2B in France, B2C in Italy, other countries following in the next years) ■ No internal usage so far (secure own authentication available already) ■ B2B2C transactions, with the objective to include digital signature in the applications of Credit Agricole partners (e.g. put the digital signature in the checkout of an e-commerce website)
Benefits gained	■ Increase of customer journey - Customer satisfaction due to being perceived as innovative ■ Lower cost expected in the next years compared to paper-based approach ("will definitely pay off in the near future")
Challenges	■ Took time to guarantee a good customer journey (the whole workflow – not only digital signing – had to be transformed) ■ Clarification of legal validity needed effort (legal advisory was needed) ■ High initial cost to adapt industrial process
Main criteria for supplier choice	■ Legally valid solution ■ Collaborative partnership ■ Technical expertise
Key considerations when choosing supplier	■ Legal validity of solution and legal advisory by supplier possible ■ Standardized solution for a European-wide deployment

2 Information gained through interview with Credit Agricole/CA Consumer Finance - representative

Conclusion

The technology of digital signature will be present in many areas of our daily life where confidentiality is involved. The technology brings higher business efficiency and cost savings, and will be increasingly adopted as a communication tool by business partners, customers and public authorities. As for every relatively new technology, hurdles have to be overcome, such as the ease of integration and alignment with existing workflows, the business case calculation as well as the lack of transparency and often misunderstanding of the legal situation. With the new EU regulation expected to be implemented this year promoting the overall legal validity as well as acceptance of cloud-based solutions, there are already very promising signs that authorities and the supplier industry are overcoming these challenges. As the market demands a quick return on investment and a solution that is facilitating workflows, full or partly cloud-based solutions are expected to take a major part of the digital signature solution market in the future. Those who realize the potential of such solutions now will be able to create significant cost advantage, as well as better maintain and expand their customer base due to the higher convenience of these solutions.

Contacts

If you would like more information or to arrange an informal discussion on the issues raised here and how they affect your business, please contact:

Austria
Karim Taga
taga.karim@adlittle.com

Belgium
Gregory Pankert
pankert.gregory@adlittle.com

China
Antoine Doyon
doyon.antoine@adlittle.com

Czech Republic
Dean Brabec
brabec.dean@adlittle.com

France
Didier Levy
levy.didier@adlittle.com

Germany
Michael Opitz
opitz.michael@adlittle.com

India
Srini Srinivasan
srinivasan.srini@adlittle.com

Italy
Giancarlo Agresti
agresti.giancarlo@adlittle.com

Japan
Shinichi Akayama
akayama.shinichi@adlittle.com

Korea
Kevin Lee
lee.kevin@adlittle.com

Latin America
Vincenzo Basile
basile.vincenzo@adlittle.com

Middle East / Malaysia
Thomas Kuruvilla
kuruvilla.thomas@adlittle.com

The Netherlands
Martijn Eikelenboom
eikelenboom.martijn@adlittle.com

Nordic
Martin Glaumann
glaumann.martin@adlittle.com

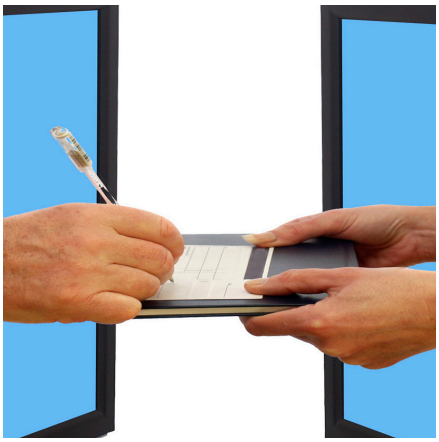
Singapore
Yuma Ito
ito.yuma@adlittle.com

Spain
Jesus Portal
portal.jesus@adlittle.com

Switzerland
Clemens Schwaiger
schwaiger.clemens@adlittle.com

UK
Richard Swinford
swinford.richard@adlittle.com

USA
John Brennan
brennan.john@adlittle.com



Arthur D. Little

As the world's first consultancy, Arthur D. Little has been at the forefront of innovation for more than 125 years. We are acknowledged as a thought leader in linking strategy, technology and innovation. Our consultants consistently develop enduring next generation solutions to master our clients' business complexity and to deliver sustainable results suited to the economic reality of each of our clients.

Arthur D. Little has offices in the most important business cities around the world. We are proud to serve many of the Fortune 500 companies globally, in addition to other leading firms and public sector organizations.

For further information please visit **www.adl.com**

www.adl.com/DigitalSignature