Remote e-identification and e-signatures

Trusting someone you have never seen

Stéphane Hurtaud
Partner
Cybersecurity Leader
Deloitte

Irina Hedea
Director
Risk Advisory
Deloitte

Ismaël Cissé
Senior Manager
Risk Advisory
Deloitte
Over the past 20 years, the rise and rapid evolution of information and communication technologies has led to new digital services and usages responding to customers’ need for mobility, convenience, efficiency and rapidity in the services response time. In the banking industry for example, this evolution was reflected by the development of services such as online and mobile banking and their rapid adoption by the customers.

However, as these new electronic services grow in magnitude, the risks related to cybercrime, identity fraud and leakage of personal data are also increasing. As a consequence, many organizations have the same concerns:

• How can I ensure the identity of a counterpart (natural or legal person) during an electronic transaction?
• How can I perform digital business or administrative transactions in a convenient, secure and seamless manner while maintaining the legal value of these transactions?

In this context, allowing citizens and businesses to identify remotely when performing electronic transactions is key for answering this need for mobility and convenience. Consequently, the digital world needs to be protected by strong security measures.
Use case and challenges
Part of the trust in the digital world, remote electronic identification is the process of identifying a person only based on data in electronic form, without any face-to-face meeting.
In the financial sector, remote electronic identification supports a wide variety of use-cases, for example, the bank account opening or the online credit subscription. Such a solution typically involves several stakeholders:
• The provider of the remote electronic identification technology, solution or platform
• The provider of the service itself, such as the bank for an online bank account opening

For example, opening a new bank account can be done if a person is physically within the bank’s premises or if the bank provides the required technologies for proceeding with this service remotely.

Independently of how the account is opened, a process involving different checks related to “Know your customer” (KYC) and “Anti money laundering” (AML) has to be performed. Documents such as ID card or passport, proof of residence, employment contract and client’s consent for terms and conditions have to be presented and validated. The client’s signature on the contractual agreement also has to be received.

Electronic identification allows this process to be performed remotely and from any location, provided that the client has, among others, an internet connection (e.g. from the client’s home or office):
01. The client connects to the bank’s website and initiates the account opening process
02. Then, he/she provides the requested personal information and supporting documents online
03. He/she is then invited to download an application, based on which the remote
electronic identification is performed: A trained expert performs a live-video identification of the client (face verification and cross-checking with ID card).

After the remote electronic identification, the bank performs the verification of the provided documents and, should the results of the controls be successful, opens the account.

As a conclusion, for the same process, the remote electronic identification allows an increase in efficiency and rapidity while keeping the same level of trust.

Further examples can be given, in different industries, such as online life insurance subscription, online telephone subscription, online apartment, and house rent subscription etc.

**Information security challenges**

For providing the required trust during a remote electronic identification, ensuring the security of the data exchanged through Internet is mandatory. Consequently, the solutions and processes supporting the remote electronic identification have to be securely designed, implemented, and operated in order to ensure the confidentiality, integrity, and availability of these data. Appropriate security measures must be adopted to reduce risks such as data leakage and identity fraud.

**Legal challenges – Focus on eIDAS and qualified trust services**

Another challenge for ensuring trust is to use the remote electronic identification solutions that are aligned with the different regulations currently applicable for the digital services.

Depending on the risks related to the remote electronic identification and the legal value expected from the digital service, the regulation currently applicable is the European regulation (EU) No 910/2014 (the “eIDAS” regulation). The eIDAS regulation addresses the cross-border harmonization at the European level of the legal value of trust services such as electronic signatures, electronic seals, electronic time stamps, electronic registered delivery service, and website authentication.

The regulation also defines the status of qualified trust services, which benefit from the presumption of reliability in legal proceedings. In the specific case of the qualified electronic signatures, the regulation goes even further by bestowing a qualified electronic signature the equivalent legal effect of a handwritten signature.

In this context, a third player comes into the ecosystem: the Trust Service Provider, which provides a trust service (e.g., an electronic signature certificate) to the user at the end of the remote electronic identification process. In the context of the online bank account opening, this could allow the client to electronically sign a contract at the end of his remote electronic identification, which would successfully conclude the client on-boarding process.

The eIDAS Regulation in its article 24 addresses the requirements related to the remote electronic identification process for enabling the delivery of qualified trust services:

> “1. When issuing a qualified certificate for a trust service, a qualified trust service provider shall verify, by appropriate means and in accordance with national law, the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate is issued.

The information referred to in the first subparagraph shall be verified by the qualified trust service provider either directly or by relying on a third party in accordance with national law:

a. by the physical presence of the natural person or of an authorised representative of the legal person; or

b. remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels ‘substantial’ or ‘high’; or

c. by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b); or

d. by using other identification methods recognized at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body.”

In this context, in order to provide the highest level of trust, the main challenge for remote electronic identification providers and Trust Service Providers is to ensure that their identification methods (e.g. live video identification) are recognized at national level as providing an equivalent assurance as the physical presence.

**Operational and technical challenges**

Organizations choosing to benefit from remote electronic identification are also facing operational and technical challenges. They have to select secure and technically mature solutions to provide the best service to their customers; however, this is just the tip of the iceberg.

Other key considerations are the technical integration of the solution in the existing infrastructure and processes while assessing the organizational changes towards their employees, clients and partners this integration will create.

The solutions provided by remote electronic identification providers, supported by the Trust Service Providers try to tackle the challenges previously mentioned, while ensuring the quality of the digital services.

---

Remote electronic identification allows processes such as bank account opening and credit subscription to be performed remotely and from any location, provided that the client has an internet connection.

A vision of the remote electronic identification market
Analysis of the market
The remote electronic identification market is still emerging. This can be explained by the fact that the technologies used to perform the remote electronic identification are quite recent. In addition, the capability to meet the requirements of the digital services regulations (e.g. eIDAS), when applicable, is in its infancy.

However, from a technological perspective, video quality (particularly on mobile devices) and network bandwidth are now efficient, thus paving the way to creating a strong technological market in the mid-term.

In order to benefit from the added value related to trust services such as the electronic signatures, the remote electronic identification providers couple their solutions with services from Trust Service Providers such as LuxTrust, Namirial or Infocert.

A good example of collaboration between a remote electronic identification provider and a Trust Service Provider is the one between IDNow and LuxTrust for the provision of added-value services such as the online bank account opening.

Diversification of Trust Service Providers’ services
In the context of a remote electronic identification enabling the delivery of trust services, the eIDAS regulation states in its article 13 that “Without prejudice to paragraph 2, trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation.”

Consequently, for having a competitive advantage in the digital market, Trust Service Providers need to demonstrate that they meet the eIDAS regulation’s requirements, need to obtain the related certifications and to ensure the information security.

Since eIDAS provides a pan-European framework for mutually accepted identities, this represents an opportunity for Trust Service Providers to diversify their service offering as a one-stop-shop for supporting remote electronic identification, identity management, authentication and electronic signing solutions.

Example of differentiators
As in every new market, it is key for providers to identify the features which will allow their solutions to differentiate from others. In the context of remote electronic identification, the following aspects can be considered as differentiators:

• User experience
• Compliance with applicable legislations (e.g. eIDAS, GDPR and PSD2 for payment services) and related certifications
• Information security
• Re-usability of the identification process for other added-value services allowing for data portability and gain in time and costs (as one avoids repeating the identification procedures)

Multi and omni-channel service (available on any type of device or platform)

These differentiators in general, will drive partners and clients to trust the digital services offered and will open the way for a swift and steadily growing adoption of remote electronic identification.

2. eIDAS article 13, paragraph 2 “Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations.”
Conclusion

Remote electronic identification is not a new topic. However, the key challenges that should be addressed while offering the expected quality, efficiency and legal value are becoming more and more significant.

Nevertheless, the legal framework introduced by eIDAS (such as the qualified trust services) allows leveraging on digital services that sustain the cross-border digital market in a trusted, innovative and efficient manner.

Organizations choosing to implement added-value services based on remote electronic identification have now the ground towards a digital transformation in a trusted and secured environment. Their journey can start right now.