CLIFFORD
CHANCE

Briefing note March 2017

Electronic trust services: risks and advantages in business transactions

The EU Regulation on electronic identification and trust services ("**eIDAS**" Regulation, no. 910/2014), which came into effect on 1 July 2016, has introduced a set of electronic trust services to give legal certainty and reliable identification in the context of **electronic transactions**.

In addition to electronic signatures, which ensure well-know advantages in terms of legal certainty of the signature and execution by parties or their representatives no matter where they are in the world, eIDAS provides for:

- **electronic seals**, which give evidence (i) that the electronic document originates from a legal person and (ii) of the authenticity and integrity of the electronic document's content, because any subsequent change in the document will be detectable;
- **electronic time stamps**, which ensure the legal evidence of the date of creation of the electronic document.

Making the right choice

Electronic trust services, i.e., electronic signatures, electronic seals, and electronic time stamps, are of service for businesses that manage a significant amount of electronic documents, by ensuring legal certainty and saving time and costs. Organisations should choose the right trust services for their objective: whether, among others, **to provide certainty as to the date of execution of an electronically executed contract**, including for the purposes of "***date certain***" under Italian law, as well as **to have evidence that the document was truly originated by a specific company or organisation, for example to reduce the risk of "phishing"**. To achieve these objectives, operators should procure that they implement electronic trust services in compliance with the requirements under EU and domestic regulations. Moreover, operators should be mindful of the risks related to the increasing use of electronic trust services in terms of cyber security and data protection.

The eIDAS provides for subsets of electronic trust services that ensure increasingly stronger legal effects, such as qualified electronic seal ("**QES**")[1] and qualified electronic time stamps ("**QETS**")[2] . QETS and QES grant specific legal presumptions because they are issued by trust service providers that have been awarded qualified status by a EU member State supervisory body. The EU Commission makes available the member States trusted lists of qualified trust service providers; in Italy supervisory body responsible for the list is the *Agenzia per l'Italia Digitale* (Agid).

[1] Under Article 3(27) of the eIDAS, a qualified electronic seal is an advanced electronic seal based on a certificate issued by a qualified trust service provider.
[2] Under Article 42 of the eIDASm QETS are executed through an advanced electronic signature or an advanced electronic seal of a qualified trust service provider.

How it works

Electronic seals are unique data that identify the entity issuing the electronic seal and are associated to the content of an electronic document. Electronic seals can be executed by means of different procedures and tools. For example, electronic seals can be executed by means of smart cards activated through a pin code. When organisations need to have a large amount of documents sealed, several people can be given access to the sealing system, for example by means of personal pin codes. Moreover, mass sealing cards allow the execution of the electronic seal on a large scale.

The EU Trust Mark allows easy recognition of service providers with qualified status.

Electronic time stamps are not specific tools or devices but rather the result of a procedure that ensures the relevant date/time of the electronic document.

A person requiring an electronic time stamp is provided with a system-software ensuring the following quick steps:

1. the file's fingerprint, which is a code uniquely identifying the file (also known as hash code), is sent to the time stamp provider;
2. the time stamp provider certifies the fingerprint and its date/time, for example by applying its digital signature to them;
3. the certified fingerprint is sent back to the person having requested the time stamp. Concretely, what is received is a certificate stating the relevant electronic document's date/time.

Advantages

- Electronic trust services ensure significant savings of **time and costs** in the context of high-volume and cross border transactions, making concurrent execution of a document possible regardless of where in the world the signatories are.

Key issues

- Electronic trust services enjoy cost and time saving and their legal effects should be recognized before any EU member State court.
- The option for the right electronic trust service is material for business operators in order to ensure the specific legal effects necessary to secure the electronic transaction.
- Cyber security and data protection risks must be effectively faced to make an electronic transaction system profitable.

- Companies and organisations that process a large number of electronic documents, such as leasing companies, banks and public institutions, can use **QES** to seal these documents through **automated processes**.
- Electronic seals and electronic time stamps, as well as electronic signatures, are **admissible as evidence** in the courts of any EU Member State.
- Use of **QETS** gives the benefit of the **presumption of accuracy of the date and the time** of the related electronic documents. Companies and organisations can rely on the fact that the *"date certain"* of their electronic documents cannot be challenged before any EU Member State court, other than on the basis of the specific evidence that the electronic document was not executed on the date/at the time indicated by the QETS.
- The use of **QETS** and **QES** also gives rise to a **presumption of the integrity/authenticity** of the contents of the related electronic documents, because QETS and QES ensure that the content of an electronic document has not been changed after the execution of the QETS or QES.

Risks

- The use of non-qualified electronic time stamps may expose companies and organisations to the risk that the date of their electronic documents be challenged. In Italy, ***"date certain" ("data certa")* is a material issue in litigation**: for example, in accordance with established case law, the lack of *"date certain"* may prevent a creditor from having its receivables admitted

as a liability of the debtor in the context of the debtor's insolvency proceedings. The lack of *"date certain"* can evolve into a systemic risk for companies and organisations that manage both electronic and handwritten contractual documents, where the signatures are not notarized or where *"date certain"* is not otherwise ensured (such as by filing the contract with the Companies Register).

- Use of electronic trust services may increase exposure to cyber risk and therefore to **fraud and data loss**. The 2017 report from Clusit – Italian Information Security Association stated that, in 2016, the number of cases of cybercrime and cyber warfare[3] in Italy was the highest over the last six years, with cyber attacks/cybercrime increasing by 9.8% and cyber warfare increasing by 117%[4]. In 2016, **cyber attack cases** increased particularly in the **large-scale retail** sector (by 70%) and in the **banking and finance** sector (by 64%).

  To face the cyber threat, it is likely that **business operators will be called to implement higher security standards in their network and information systems** over the next few years. The EU NIS Directive[5], approved on 6 July 2016, binds member States to ensure that operators of essential service[6] , such as in the **energy, transport, banking, and health sectors**, implement technical and organisational measures to handle the risks posed to the security of network and information system. The NIS Directive must be enforced by EU member States by 9 May 2018.

  The cyber security issue is also material in light of financial institutions' increasing investments in artificial intelligence and in new technologies aimed at managing big data processing.

  Opting for services from qualified trust service providers may be one a step towards ensuring a higher level security as well as more legal certainty with regards to electronic documents.

- The use of electronic trust services involves the transfer and storage of a large volume of data, which may expose companies and organisations to significant **confidentiality and data protection risks**:

  (a) as for **confidentiality risk**, electronic seals do not prevent electronic documents from being accessible to unauthorised parties. For this reasons, specific encryption solutions should be implemented, with the support of qualified trust service providers, when transactions need to be secured from a confidentiality standpoint;

  (b) as for **data protection risk**, under Article 37, paragraph 1(a), of Legislative Decree 196/2003, a company or an organisation controlling personal data because of the use of electronic trust services may be required to file a preliminary notice with the Italian Data Protection Authority; for example, where the implementation of advance electronic signature systems may involve the collection of biometric data such as graphometric signatures[7].

  The control of massive personal data may give rise to some concerns also under article 36 of new EU Data Protection Regulations[8], which will come into force on 25 May 2018 and will create a specific obligation, for the personal data controller, to consult the relevant data protection authority when the data protection impact assessment indicates that the data processing would result in high risk and the controller has not implemented specific measures to mitigate this risk.

  Specific encryption solutions and the support of qualified trust service providers might help to mitigate some of the concerns related to personal data processing.

Towards a balance

Electronic trust services represent a good opportunity for business operators to simplify processes while at the same time increasing the processes' reliability. These objectives

[3] Cyber warfare is defined in Cambridge dictionary as "the activity of using the internet to attack a country's computers in order to damage things such as communication and transport systems or water and electricity supplies".
[4] Source: Sole24Ore, at the following url http://www.infodata.ilsole24ore.com/2017/02/22/cybersicurezza-2016-da-incubo-e-stato-lanno-peggiore-di-sempre.
[5] EU Directive concerning measures for a high common level of security of network and information systems across the Union, no. 1148/2016.
[6] Under Article 5, paragraph 2, of the NIS Directive, an operator provides essential services when it meets the following requirements: (a) an entity provides a service which is essential for the maintenance of critical public and/or economic activities; (b) the provision of the service depends on network and information systems; and (c) an incident would have significant disruptive effects on the provision of that service.
[7] Graphometric signatures are handwritten signatures executed by means of a tablet using a special pen or a smartphone and being added to a digital document.
[8] EU Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, no. 679/2016.

can be reached only if an effective risk assessment is performed case by case.

Both legal and technical issues should be taken into consideration to balance the need for legal certainty with the need to simplify corporate processes without jeopardising effective risk management.

For example, to enter into a large number of standard agreements with customers, it may find more profitable for companies to use less sophisticated tools, such as starting the process by way of advanced electronic signature (e.g. graphometric signature) and then securing the electronic agreements by implementing an internal QES or QETS execution step. On the contrary, for the electronic execution of high-volume transactions, the use of more sophisticated tools such as electronic signatures based on certificate issued by qualified trust service providers may be required toghether with QETS or QES.

Contacts

Carlo Felice Giampaolino
Partner

T: +39 06 4229 1356
E: CarloFelice.Giampaolino
@cliffordchance.com

Francesco Panetti
Senior Associate

T: +39 06 4229 1260
E: Francesco.Panetti
@CliffordChance.com

Alessandro Sciarra
Associate

T: +39 06 4229 1384
E: Alessandro.Sciarra
@CliffordChance.com