ELECTRONIC TIMESTAMPING

White Paper

Date of first publication 1st April 2021

Abstract

Vaultinum provides physical and electronic timestamping services as part of its activities as a trusted service provider, particularly for the deposit and archiving of digital assets or records.

1st April 2021

INTRODUCTION

It has been customary throughout the centuries to record events and all related information, notably the date of the event, in registers. Record-keeping has been an essential element in the development of organized human societies. Thus, already in ancient Rome, bankers chronologically recorded all deposit and withdrawal transactions in their registers.[1] The same applied to auction records, trade records, and others. The Templars used similar registers in the 12th and 13th centuries and even created a secret code verification system that allowed pilgrims to travel without having to carry any belongings, goods or cash on their person.[2] In the 9th century, the ancestor of the banknote, called "flying money" or "Fey-thsian", made its appearance under the Tang dynasty and involved a system of deposit registers and dated receipts.[3] In 14th-century France, the Church established the use of parish registers, precursors of civil registries, in which baptisms, marriages and burials were recorded and dated and which were often used as evidence during trials.[4]

The practice of associating a date or even a time with an event or a document, also called "timestamping", has its roots in the need to produce evidence to assert or confirm a right or an obligation during a dispute or litigation. Administrations often ask citizens to provide an extract of a birth certificate not older than three months. The reason for this request is not related to the birth as such, but to the person's status at the time of the request. Indeed, the birth certificate also mentions important events creating rights or obligations (marriage, divorce, civil partnership, guardianship, etc.). The affixing of the stamp and the date by a registrar on the extract provides this proof.

But how do you verify the existence of electronic data? The digitization of entire sectors of economic activity has led to the need for electronic timestamping, to verify both timing and content. In many areas such as intellectual property, personal data protection and IT, it has become essential to prove the existence of specific data at a specific date and time. In the

[1] Maud MARCHAND, *La comptabilité à Rome sous la République et au début de l'Empire*, Ecole Nationale Supérieure, 2006.
[2] William Goetzmann, *Money Changes Everything*, Princeton University Press, 2017.
[3] Banque Nationale de Belgique, Le billet, une invention chinoise?
[4] Wikipedia, *Histoire de l'état civil en France*.

absence of such proof, a person could be denied rights which are rightfully theirs and/or be wrongly penalised.

However, electronic timestamping raises new questions, notably as to the reliability of the process. The debate on the probative value of emails is still recent. Everyone knows how easy it is to change the local time on a computer or a computer system. Consequently, a new law had to be introduced to regulate electronic timestamping systems and thus set certain technical requirements to guarantee their reliability as evidence.

1. PRESENTATION OF ELECTRONIC TIMESTAMPING

1.1 What is electronic timestamping?

All computer systems are equipped with a real-time clock which indicates the current date and time for various operations carried out on the device, such as creating a file or sending an email. These clocks keep accurate time even when the device is turned off, because not only are they powered by a battery located on the computer's motherboard, but they are also connected to the Internet. As such, this internal computer clock already provides a form of electronic timestamping, but it is unreliable. Not only can we manipulate the date and time within the software, but we can also tamper with the system clock to change the date and time associated with records in the event logs, the file system or in database transactions.

To achieve the reliability provided by the registrar stamping a certificate, the initial regulations called for the participation of a trusted third party in the electronic timestamping process. Timestamping was defined for the first time in article 1 of the decree of 20 April 2011[5] as the "*mechanism associating a representation of data at a particular time and attesting to the existence of the representation of this data at this instant by means of a timestamp token [which] includes a stamp from the electronic timestamping service provider established using the signature data of the timestamp token*". This definition of electronic timestamping therefore presupposes the use of a trusted service provider, which de facto excludes certain forms of electronic timestamping.

A few years later, in 2014, the European Union regulation on electronic identification and trusted services for electronic transactions in the internal market, known as the eIDAS regulation, was adopted. It aims to allow the free circulation of timestamp tokens and therefore facilitate trade for more than 400 million people. In this regulation, electronic timestamping is defined more largely as "*data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time*".[6]

In other words, ***electronic timestamping is a process whereby a date and time can be electronically bound to other data in electronic form to certify, either with or without the intervention of a trust service provider, of its existence or execution at a given moment*** **and also to attest to its content at that precise time.**

Vaultinum has long been providing physical and electronic timestamping services as part of its activities as a trusted service provider, particularly for the deposit and archiving of digital assets or records.

1.2 What are the two recognized types of electronic timestamping?

The eIDAS regulation mentions two categories of electronic timestamps:

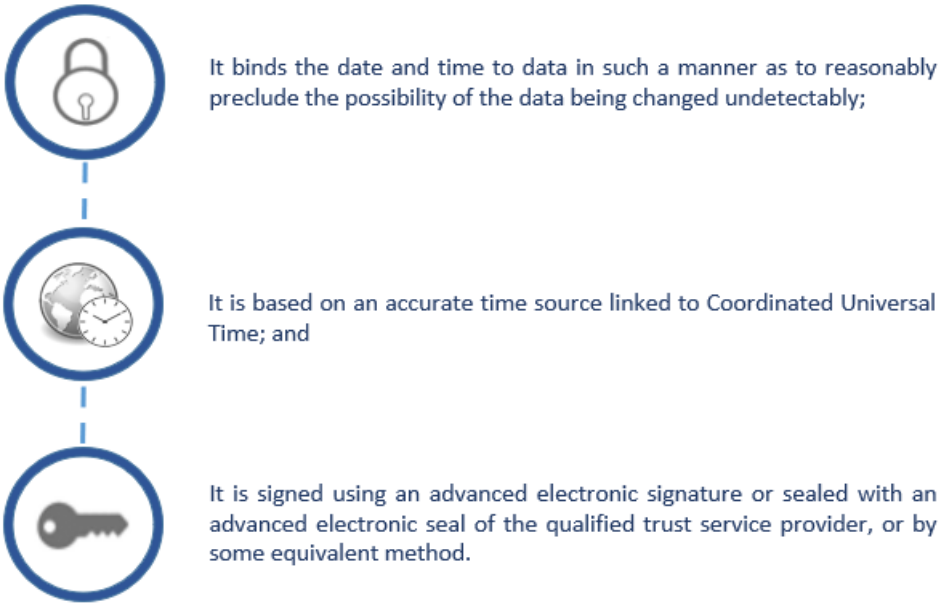
- Non-qualified or simple electronic timestamping;
- Qualified electronic timestamping.

The regulation does not provide a specific definition for simple electronic timestamping. It is understood that a timestamping process that does not meet the conditions indicated in the eIDAS regulation is of the non-qualified type.

[5] Decree No. 2011-424 of April 20, 2011 relating to the time stamping of mail sent or received by electronic means for the conclusion or performance of a contract.

[6] Regulation (EU) 910/2014 of 23 July 2014 on electronic identification and trusted services for electronic transactions within the internal market and repealing Directive 1999/93/EC, art. 3§33.

Conversely, article 42 defines qualified electronic timestamping as fulfilling the following conditions:



Regarding this last condition, the eIDAS regulation leaves room for innovation and the development of a method ensuring a level of security equivalent to the advanced electronic signature or the advanced electronic seal. It is up to the trust service provider to demonstrate that its method meets the requirements set out in the eIDAS regulation.[7]

1.3 How does electronic timestamping work?

Electronic timestamping (with use of a trust service provider) is a "process which links the representation of a data to a particular time". To apply a timestamp to data in electronic form (example: a contract, software source code, an invoice, an electronic medical prescription, a price indication, a ticked box on a form, access to an information system), a unique identifier must be generated through use of the hash function. This step is essential in order to create a reliable and unique representation of the data; that is, a virtual fingerprint. This is then transmitted to the timestamping service authority, which **combines the digital fingerprint with the exact date and time based on Coordinated Universal Time (UTC).** The reliability of this combination is guaranteed by means of a timestamp token, which is a type of signed certificate containing:

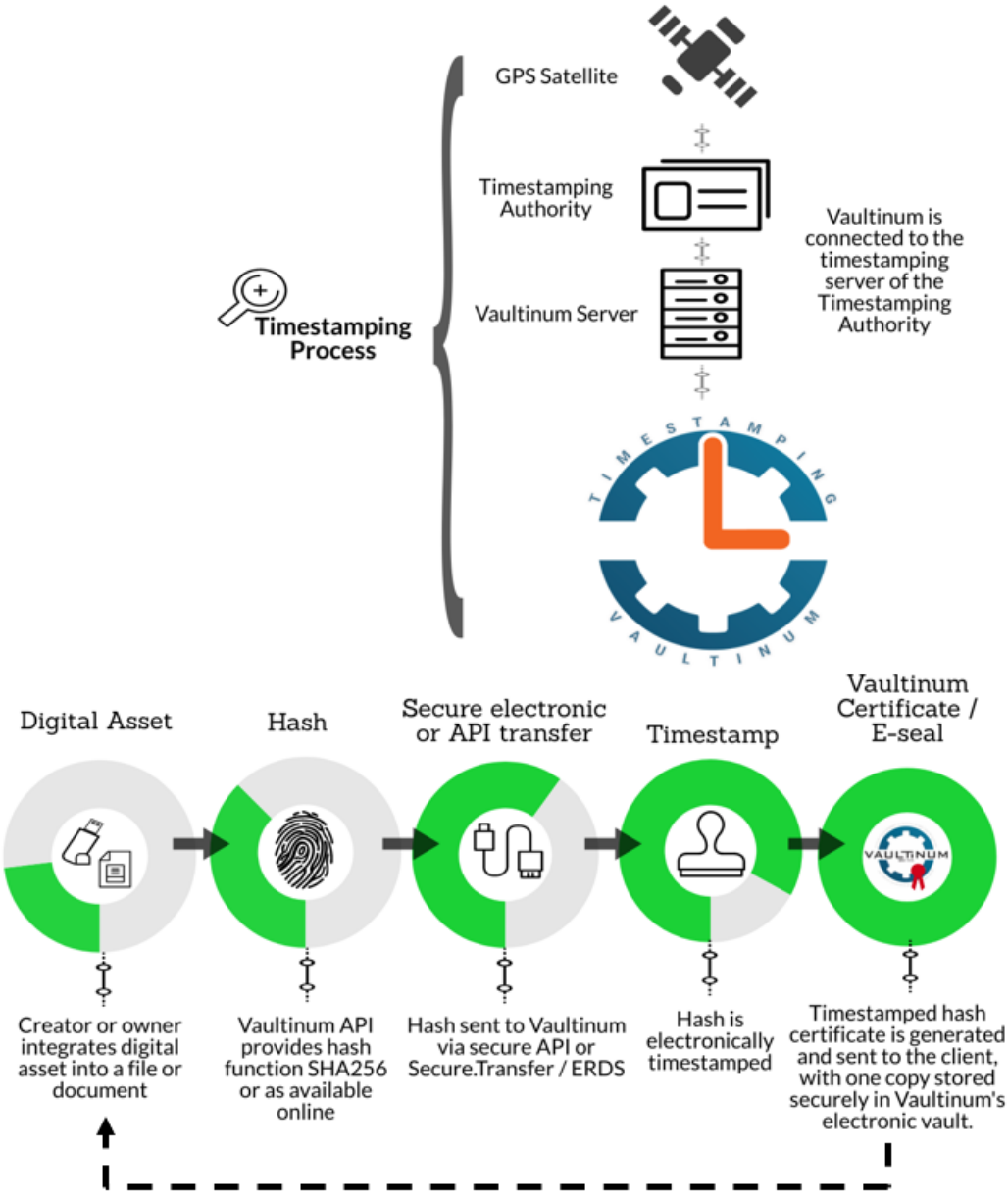
- the digital fingerprint or representation of the data;
- the UTC date and time;
- the timestamp token seal.

Under the French decree on electronic timestamping, the timestamp token seal allows the identification of "*the electronic timestamping service provider that issues it and ensures a link with the timestamp token to which it is attached*." It is the combination of the timestamping authority's private key and a public key, communicated to the user by means of an electronic certificate.[8]

[7] Regulation (EU) 910/2014 of 23 July 2014 on electronic identification and trusted services for electronic transactions in the internal market and repealing Directive 1999/93/EC, recital 62.

[8] Thierry PIETTE-COUDOL, *Fiabilité de la date et horodatage de l'article 1369-8 du Code civil*, Revue Lamy Droit de l'Immatériel, n°72, 1st June 2011.

At the end of the timestamping process, the timestamping authority sends all these items to the user and also archives them.



2. THE LEGAL ADMISSIBILITY OF ELECTRONIC TIMESTAMPING AS EVIDENCE

2.1 The legal admissibility of electronic timestamping as evidence

Timestamps, even when electronic, are admissible as evidence in the courts of the European Union.

Thus, a non-qualified electronic timestamp is admissible in court, in particular when evidence can be produced by any means. In point of fact, article 41§1 of the eIDAS regulation establishes a principle of non-discrimination as regards electronic timestamping, accepting it as evidence in court at the same level as manual timestamping, even if it does not meet

the requirements of qualified electronic timestamping.[9] The same holds true for non-qualified electronic registered delivery services.

In Switzerland, the SCSE regulation of 2016 provides a legal framework that is similar to eIDAS. Although SCSE does not provide specifications on the technical standards that need apply, the Swiss Federal Council recognizes as valid, processes that have been implemented in line with eIDAS standards. As with eIDAS, SCSE grants a higher probative value to certificates issued by qualified trust service providers.

2.2 Presumption of reliability in favor of qualified electronic timestamps

Contrary to the simple electronic timestamp, **a qualified electronic timestamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound** (article 41§2 of the eIDAS regulation). This provides a significant advantage in the event of litigation or dispute, as ***it allows to reverse the onus of proof***[10] and the burden of proof can be shifted onto the party challenging the reliability of a qualified timestamping system. In this context, a part of the doctrine equates qualified electronic timestamping with the electronic version of the legal concept of "certain date"[11].

By extension, in France, article L100 of the postal and electronic communications code states that electronic registered delivery is the equivalent of physical registered mail as long as it meets the requirements of article 44 of the eIDAS regulation, especially as regards the use of a qualified electronic timestamp. In this case, the data sent and received by means of a qualified electronic registered delivery service benefits, among other things, from a presumption as to the integrity of the data and the correctness of the date and time of sending and reception.[12] In fact, an electronic timestamp applied to registered mail has an advantage over physical registered mail, because electronic timestamping not only certifies the date but also the content, which physical registered mail does not.

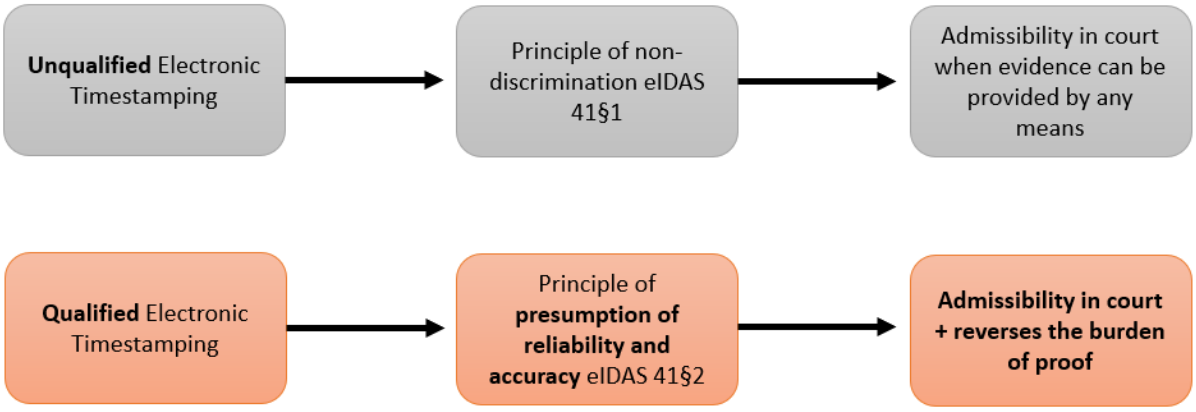
Thus, when the Vaultinum timestamps electronic documents such as an invoice, a reference price or a deposit, the Vaultinum stamp both provides a certain date to the documents in question as well as attests to their content at the time of affixing the timestamp token. As such, this content cannot be altered.

[9] Regulation (EU) 910/2014 of July 23, 2014 on electronic identification and trust services for electronic transactions within the internal market and repealing Directive 1999/93/EC, art. 41§1: "*An electronic time stamp shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic time stamp*."

[10] The burden of proof is the procedural obligation on a person to prove that a proposition made by that person is true or false, as the case may be.

[11] Thierry PIETTE-COUDOL, *Fiabilité de la date et horodatage de l'article 1369-8 du Code civil*, Revue Lamy Droit de l'Immatériel, n°72, 1st June 2011.

[12] Regulation (EU) 910/2014 of July 23, 2014 on electronic identification and trusted services for electronic transactions within the internal market and repealing Directive 1999/93/EC, art. 43.



2.3 Electronic timestamping and blockchain

The concept of qualified trust service providers is a crucial component of the eIDAS regulation. That being said, eIDAS does not refer to blockchain as such. It therefore remains to be seen to what extent timestamping carried out incidentally as part of a blockchain would meet the conditions for qualified timestamping. As the essence of blockchain is to eliminate trusted third parties for greater efficiency and lower transaction costs, it seems unlikely that blockchain can meet the requirements of the regulation.

Technically, blockchain technology is made up of cryptographic processes, a peer-to-peer network and timestamping functions. However, the probative value of registers using blockchain technology is far from equivalent to that of electronic timestamping systems, at least in France.

As such, it is not yet clear in France, for example, to what extent blockchain could provide proof of information. As evidence is organized and regulated by civil law, blockchain must either find its place in the existing legal framework or be the subject of specific legislation. French law of evidence is characterised by two aspects. First, it lists five different types of evidence in articles 1363 to 1366 of the Civil Code. These are: written evidence, testimony, judicial presumptions, confession and oath. Thus, it is necessary to link the information recorded by the blockchain to one of these types of evidence. Second, the probative value and admissibility of the different types of evidence are set by law. On the one hand, the legal framework determines which modes of evidence are admissible depending on the elements to be proven. Article 1358 of the Civil Code provides that "except in cases defined by law, evidence can be provided by any means". However, the law defines a great number of such exceptions. For example, as regards legal acts with a value greater than 1500 Euros, the proof must be provided in writing. On the other hand, the probative value is not the same according to the types of evidence. Only the written record, the judicial admission and the decisive oath are perceived as being perfect evidence which the judge is bound to accept. Thus, even in a situation where all types of evidence can be used, the effect will not be the same, depending on the type of evidence used. Taking into consideration that French law has long accepted digitized evidence[13], and grants digitized documents the same probative effect as physical ones on condition that "the person by whom they are issued can be duly identified and that they are created and kept under conditions such as to guarantee their integrity"[14], it is safe to conclude that there is no obstacle to defining blockchain, a digitized database, as admissible evidence. The conditions for accepting and the weight given to this digitized evidence will depend on what the evidence aims to prove. If the aim

[13] Law of March 13, 2000, which recognizes the legal value of the electronic writing under certain conditions and Order of February 10, 2016 which admits the electronic copy.
[14] Article 1366 of the French Civil Code

is to prove the date of an event, without specific legislation recognizing blockchain electronic timestamping as guaranteed data, the evidence may be admissible but its probative value would be left to the discretion of the judge.

Italy confirmed the need for specific legislation by adopting a law published on 11 February 2019 which provides that "*storing a digital document in distributed registers-based technologies shall produce the legal effects of an electronic timestamp as under article 41 of the eIDAS regulation*".[15] However, this law does not specify whether this recognition concerns only the admissibility in court of blockchain evidence as a means of proving the integrity of the document over time, or if it goes further to establish a presumption of the accuracy of the indicated date and time and the integrity of the data to which this date and time relate, in the same way as qualified electronic timestamps.

Pursuant to part of the legal doctrine, blockchain timestamping cannot, under the current state of the law, meet the conditions of qualified electronic timestamping for several technical reasons. The first is that it lacks access to an accurate time source linked to Coordinated Universal Time (article 42§1.b of the eIDAS regulation). The second is that it lacks the intervention of a qualified trust service provider (article 42§1.c of the eIDAS regulation).[16]

Finally, even if a Member State were to accept blockchain records as evidence in court proceedings, or even as providing a presumption of reliability, its laws would only be applicable within its own borders.

3. REQUIREMENTS FOR TRUST SERVICE PROVIDERS

3.1 Qualification of trust service providers

The eIDAS regulation defines the trust service provider as a natural or a legal person who provides one or more trust services. ***To be authorised to deliver qualified trust services, a trust service provider must pass a conformity assessment to confirm that it fulfils the requirements laid down in the regulation, obtain qualified status from the supervisory body (in France: ANSSI) and be identified on the trusted list published by the supervisory body.***

In practice, Article 20 of the eIDAS regulation requires qualified service providers to undergo, at least every twenty-four months, an audit carried out at their expense by a conformity assessment body. The service providers then submit the resulting report to the supervisory body within the period of three working days after receiving it. The supervisory body verifies compliance with the regulation requirements and informs the service provider of its decision.[17]

In addition to regular audits, the supervisory body may, at any time, audit or request a conformity assessment body to perform a conformity assessment of the qualified trust

[15] Legge 11 febbraio 2019, n. 12, art. 8ter §3.

[16] Actualité du droit civil du numérique, *L'horodatage électronique dans la récente loi italienne sur la blockchain : la question essentielle du temps sur la blockchain*, Revue Lamy Droit civil, n°178, 1st February 2020.

[17] Regulation (EU) 910/2014 of July 23, 2014 on electronic identification and trusted services for electronic transactions within the internal market and repealing Directive 1999/93/EC, art. 20.

service providers, at the expense of those trust service providers, to confirm that they fulfil the requirements laid down in the eIDAS regulation.

Once the trust service provider has obtained qualified status and has been indicated as such on the trusted list, ***it is authorised to use the European Union trust mark***, in accordance with implementing act n° 2015/806[18], in order to indicate in a simple, recognisable and clear manner the qualified trust services it provides.

- *Focus on France*

Wishing to provide guidance to trusted third parties, ANSSI has published two technical notes specifying, first, the qualification requirements set out in the eIDAS regulation for electronic timestamping services[19] and, second, those applicable to all qualified trust service providers[20]. Compliance with European standards ETSI EN 319 421 (formerly ETSI TS 102 023) and ETSI 319 401 as well as technical notes from ANSSI provide a presumption of conformity with these requirements. For instance, ANSSI requires timestamping service providers to preserve for a minimum of seven years after the expiry of each timestamp token, all pertinent information regarding the data issued and received, in particular for the purpose of providing evidence in legal proceedings[21].

Furthermore, if the timestamping service provider is already qualified according to the General Security Baseline (RGS), it can benefit from the terms of transition from qualification according to the RGS, to qualification according to the eIDAS regulation, as defined by ANSSI[22].

3.2 Requirements for qualified trust service providers

The eIDAS regulation sets out a number of obligations for qualified and non-qualified trust service providers. They must, in particular:

- take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide;

- notify, without undue delay, ANSSI of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data

[18] Implementing Regulation (EU) 2015/806 of 22 May 2015 laying down specifications concerning the form of the Union trustmark for qualified trust services.
[19] Agence nationale de la sécurité des systèmes d'information, *Services d'horodatage électronique qualifiés, Critères d'évaluation de la conformité au règlement eIDAS*, version 1.1, 3 janvier 2017.
[20] Agence nationale de la sécurité des systèmes d'information, *Prestataires de services de confiance qualifiés, Critères d'évaluation de la conformité au règlement eIDAS*, version 1.2, 5 juillet 2017.
[21] Agence nationale de la sécurité des systèmes d'information, *Services d'horodatage électronique qualifiés, Critères d'évaluation de la conformité au règlement eIDAS*, version 1.1, 3 janvier 2017, chapitre II.3.3.
[22] Agence nationale de la sécurité des systèmes d'information, *Services d'horodatage électronique qualifiés, Modalités de qualification selon le règlement eIDAS des services qualifiés selon le RGS*, version 1.1, 3 janvier 2017.

maintained therein. In the latter case, an additional notification can be made to the CNIL (French Data Protection Authority) or even to the person(s) concerned.[23]

Other obligations set out in the eIDAS regulation are specific to qualified trust service providers as well as to each qualified trust service they wish to provide. For example, the qualified service provider is required to:

- inform ANSSI of any change in the provision of its qualified trust services and an intention to cease those activities;
- employ staff who possess the necessary expertise, reliability and qualifications regarding security and personal data protection rules;
- have an up-to-date termination plan to ensure continuity of the service;
- maintain sufficient financial resources and/or obtain appropriate liability insurance;
- take appropriate measures against forgery and theft of data.[24]

3.3 Liability of qualified trust service providers

The eIDAS regulation provides for a liability regime for trust service providers in order to protect their customers and other persons who may suffer damage as a result of a failure on the part of the provider. Thus, under article 13§1, trust service providers, whether qualified or not, are liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under the regulation.

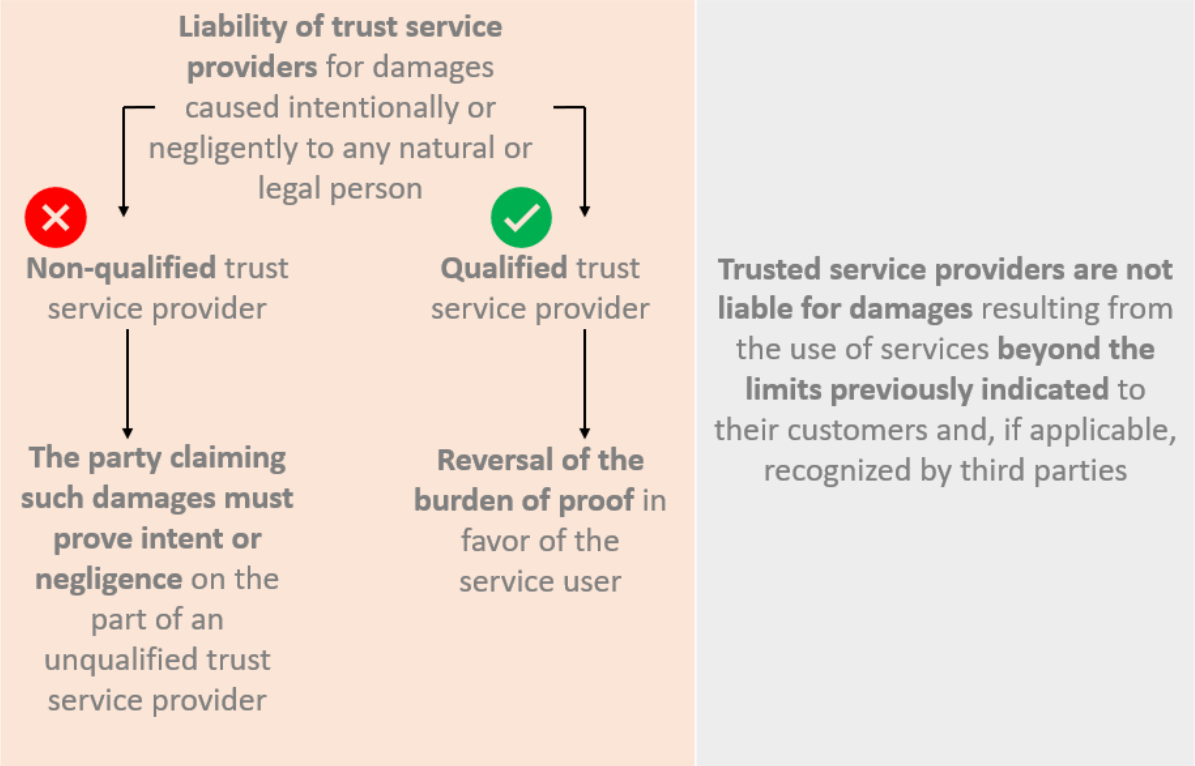
The burden of proving intention or negligence of a non-qualified trust service provider lies with the party claiming the damage.

Conversely, obtaining the qualification by a trusted third party leads, in the event of damage, to a reversal of the burden of proof in favour of the customer. As a result, in case of damage, ***a qualified trust service provider is presumed to have acted intentionally or negligently, unless it can prove that the damage was caused without intention or negligence on its part***.

However, trust service providers, qualified or not, cannot be held liable for damages resulting from the use of the services exceeding the limits previously indicated to their customers and, where applicable, recognized by third parties.[25]

By way of example, with regard to electronic registered mail, a trusted third party can be held liable and be punished with a fine of 50,000 euros if it offers or provides a service under conditions liable to mislead the sender or the recipient as to the legal effects of the delivery, thereby acting in breach of the requirements set out in article L100.[26]

[23] Regulation (EU) 910/2014 of July 23, 2014 on electronic identification and trusted services for electronic transactions within the internal market and repealing Directive 1999/93/EC, art. 19.
[24] Regulation (EU) 910/2014 of July 23, 2014 on electronic identification and trusted services for electronic transactions in the internal market and repealing Directive 1999/93/EC, art. 24.
[25] Regulation (EU) 910/2014 of July 23, 2014 on electronic identification and trusted services for electronic transactions within the internal market and repealing Directive 1999/93/EC, art. 13.
[26] Article L101 du code des postes et des communications électroniques.



4. VARIOUS USES OF ELECTRONIC TIMESTAMPING

Although electronic timestamping is mostly used when electronically signing documents, it is useful in many other areas for proof and traceability purposes. ***Vaultinum, a trusted third party, regularly provides support to its customers through its reliable, adaptable and secure timestamping system.***

4.1 Intellectual property

I developed a software. How can I protect myself against possible appropriation by a third party? How can I prove that I developed it before this third party?

According to article L111-1 of the Intellectual Property Code, "*the author of a work of the mind shall enjoy in that work, by the mere fact of its creation, an exclusive incorporeal property right which shall be enforceable against all persons.*" In other words, and subject to fulfilling certain conditions such as originality, ***copyright protection exists from the moment a work is created*** and does not require any additional formality, contrary to a trademark or an invention. This remains true throughout the 179 signatory countries of the Berne Convention.

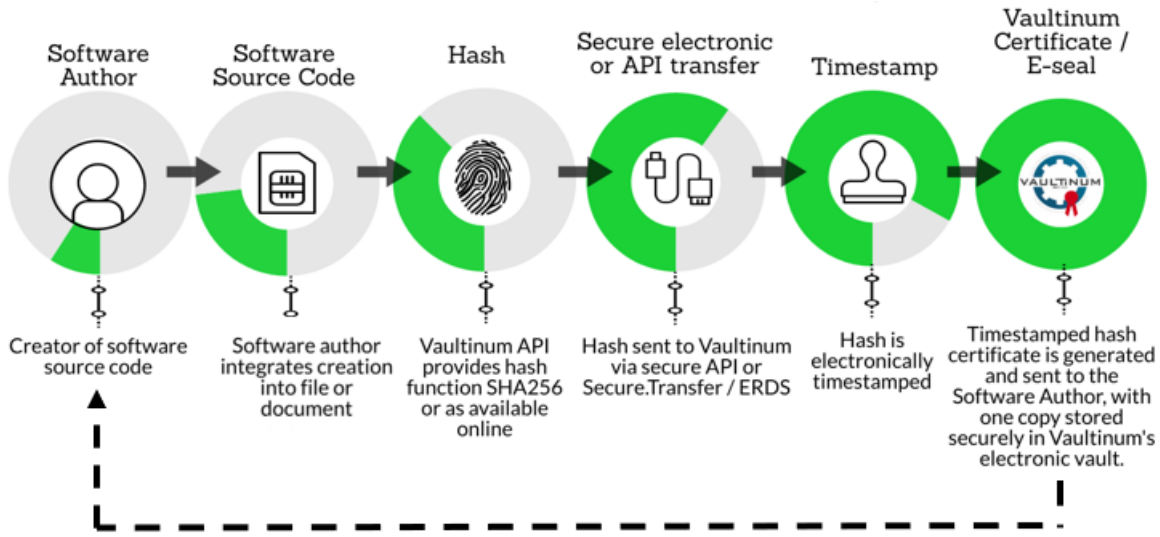
In the absence of compulsory registration with an office, it can, however, be difficult to provide proof of the existence and the content of a digital creation on a specific date, that is to say before that claimed by a possible infringer. ***It is therefore recommended to create a so-called "evidentiary repository" with a trusted third party such as a bailiff, a notary, or Vaultinum.***

Due to its technology involving the use of symmetric and asymmetric encryption algorithms, hash functions/fingerprint creation and electronic timestamping guaranteeing the integrity of the transmitted elements, the deposit made with Vaultinum:

- materialises the content of the digital creation;
- dates the creation;
- attests to the depositor's ownership;
- records the content and creation dates.

All preparatory documents necessary to file a patent application can also be filed. Indeed, the procedure for filing a patent with a patent granting authority (such as the European Patent Office, the Federal Institute of Intellectual Property in Switzerland, the National Institute of Industrial (INPI) in France, the National Intellectual Property Office in China or the United States Patent and Trademark Office) is a long and complex procedure which very often responds to the rule of "first come, first served". In this context, the evidentiary repository presents several advantages:

- It limits the risks of appropriation of an invention by partners and/or third parties;
- It affixes a date certain to ideas, projects, preparatory documents, etc. pending validation of a patent application;
- It records the results of research (especially laboratory notebooks) as and when discoveries are made so as to preserve prior rights and ensure a fair distribution of rights between employees;
- It proves that an invention kept secret was developed before a third party filed a patent on it, allowing the inventor to continue to use it (right of prior personal possession).



4.2 Personal data protection

In accordance with the GDPR, I use the email addresses of prospects to send them offers if I have their prior consent. I also delete this data three years as from the last contact with the individual concerned. In the event of a CNIL control, how can I prove my compliance with the GDPR?

- *Provide proof of consent*

In cases where the legal basis for processing is consent, the data controller must be able to demonstrate that the data subject has given consent to the processing of personal data concerning them.[27]

In practice, compliance with this obligation can be complicated as the text does not specify how this evidence can be reported. It is therefore essential for the data controller to be equipped with a tool ensuring the conservation and traceability of the following elements:

- the content and date of the consent;
- the means used to give consent;
- the information communicated at the time of consent; and
- if applicable, the date of withdrawal of consent.

On this point, the French Data Protection Authority (CNIL) indicated, in March 2017, that "*the digital timestamping of the indication of consent (by means of a click or a ticked box) and the implementation of a procedure for obtaining consent, duly documented, must be considered as a valid means of establishing proof of consent*".[28]

Vaultinum offers a reliable, adaptable and secure solution for timestamping and automated archiving thanks to its API. In addition, Vaultinum is a partner of CMP (Consent Management Platform) and as such, ensures the timestamping and, if necessary, the archiving of consent records.

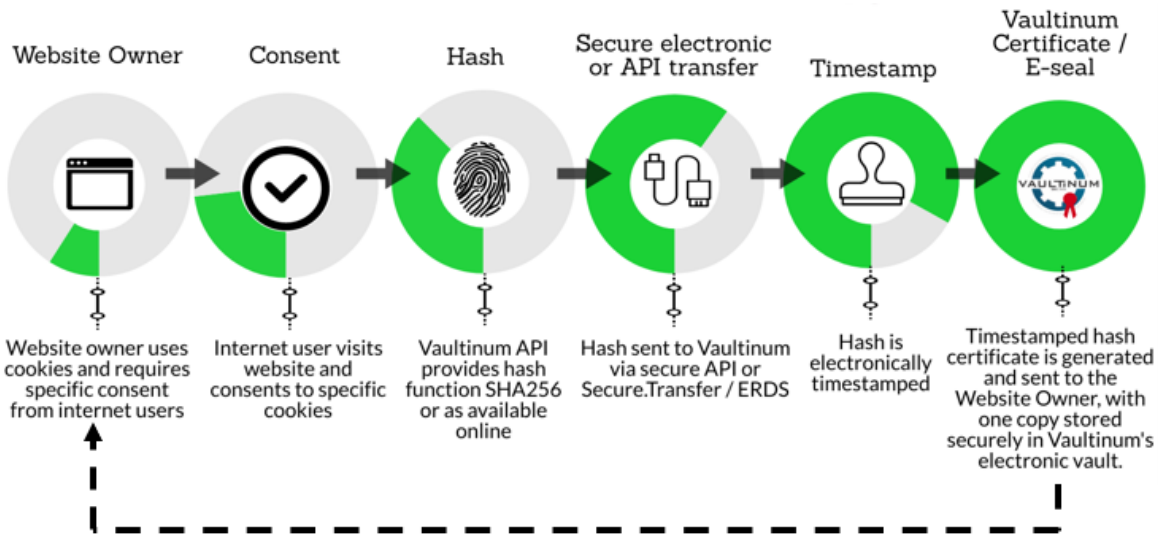
- *Providing proof of the deletion of personal data*

In accordance with the General Data Protection Regulation (GDPR), the data controller is required to determine a data retention period for each category "not exceeding that necessary for the purposes for which it is processed"[29]. The life cycle of personal data can be divided into three successive phases:

- Common or active database: the data can be used regularly by the departments involved for the time necessary to carry out the processing;
- Intermediate archiving: data is kept if there is a legal obligation or as evidence in the event of litigation, but access is restricted;

- Deletion, anonymisation/pseudonymisation or final archiving of data if they are of historical interest.

[27] Regulation (EU) 2016/679 of April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, art. 7.
[28] Commission nationale de l'informatique et des libertés, *Consultation publique sur le règlement européen*, mars 2017.
[29] Regulation (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, art. 5§1.



In order to prove compliance with the established retention periods, the data controller may use a tool to date the starting point of each phase of the data life cycle from collection to archiving/deletion.

Vaultinum provides support to its clients in setting up a timestamping system to date consent. Using the Vaultinum API, client systems can interface with the Vaultinum's timestamping solution and continuously and automatically timestamp thousands of consents in a reliable, secure and adaptable manner.

4.3 Electronic commerce

As a businessperson, I offer discounts on certain items sold on my e-commerce site. Regulations require me to justify the reference price from which the reduction is applied. How can I do this?

The authenticity of discounts offered during promotional operations is assessed with regard to unfair commercial practices (Article L. 121-2 to L. 121-5 of the Consumer Code). Price reduction announcements to consumers are governed by the decree of 11 March 2015.[30] Under article 2 of this decree, sellers are required to indicate, in addition to the announced price reduction, the reference price on the basis of which the announced reduction is calculated.

Although professionals are free to determine the reference price of their choice (for example, regular price, competitors' price, recommended price), they must be able to "*justify the reality of the reference price on the basis of which the price reduction is announced*".[31] To do this, they may use notes, slips, order forms, sales receipts, catalogues, advertising leaflets or any other documents; all the means of proof first set out in the circular of 7 July 2009 specifying the provisions of the decree of 31 December 2008 (repealed)[32]. However, these means are costly and difficult to execute, especially when price reductions

[30] Decree of 11 March 2015 relating to price reduction announcements to consumers.
[31] *Ibid.*, art. 3.
[32] Circulaire du 7 juillet 2009 concernant les conditions d'application de l'arrêté du 31 décembre 2008 relatif aux annonces de réduction de prix à l'égard du consommateur, p. 6.

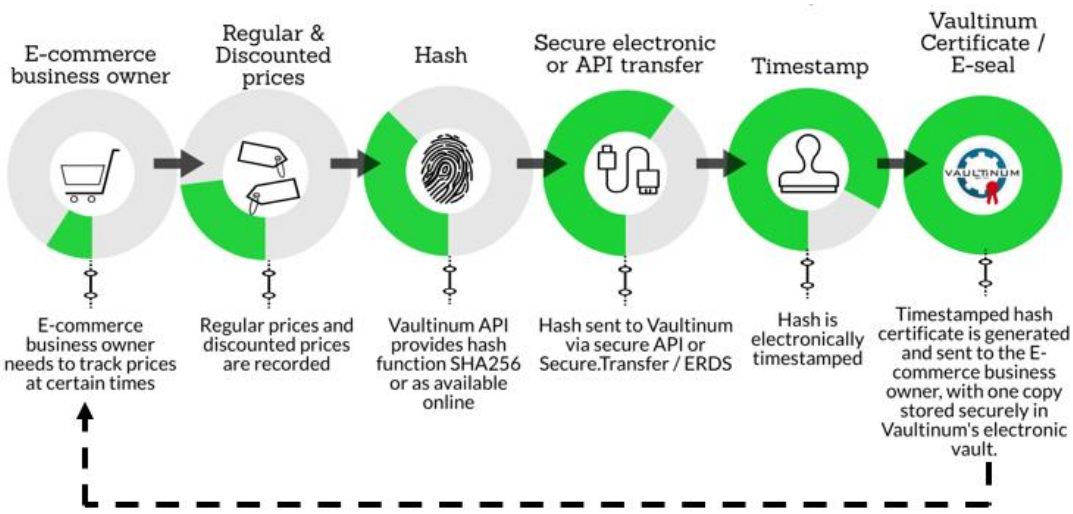
are offered online and repeatedly. They also necessitate tremendous data collection and evidence-based archiving.

With a view to limiting the impact of these regulations and simplifying the application of price reductions, professionals are recommended to use an automated timestamping tool to ensure the preservation, traceability and integrity of the following elements:

- the chosen reference price (example: price applied by a competitor);
- the location of the chosen reference price (example: a website page);
- the date of application of the chosen reference price.

The implementation of reliable and recognized means of proof to justify the reference price is all the more important as the General Directorate for Competition, Consumption and Fraud Control (DGCCRF) has for several years now, been closely monitoring online sales and particularly misleading price reduction announcements, as can be seen from its recent surveys.[33]

The Vaultinum provides support to e-commerce companies by offering them a turnkey solution for timestamping and archiving proof related to the applied reference price. Through this adaptable, reliable and secure solution, the e-merchant can connect to an API and thus manage thousands of data at a time, in an automated manner.



4.4 Information Technology

An employee repeatedly logged on to sites expressly prohibited by the company's IT charter. How can I prove this in a reliable way?

Whether human or technical, each action taken in an IT system is likely to leave tracks which must be recorded. These could be:

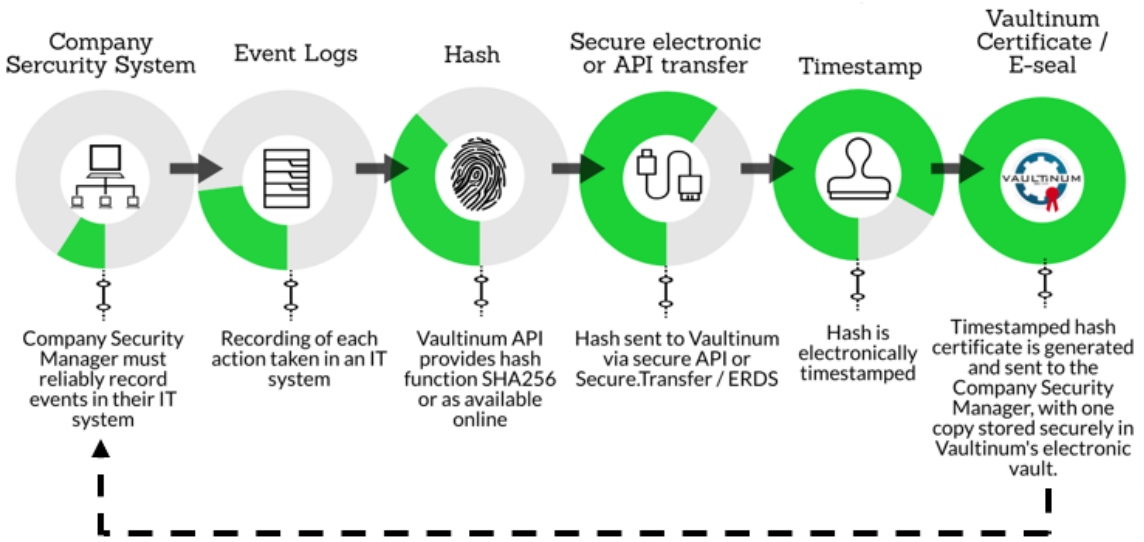
- successful connection to an application;

[33] Communiqué de presse, *Pratiques commerciales des enseignes de vente en ligne : la DGCCRF a transmis à l'autorité judiciaire les conclusions de ses investigations concernant le site vente-privee.com*, 10 janvier 2019.

- access to a file or to the internet;
- attempted intrusions into the information system;
- application requests.

The National Information Systems Security Agency (ANSSI) emphasizes that ***event logs are an essential technical component to manage the security of information systems. However, these can serve as evidence only if the log files reliably connect certain events to a particular point in time.***

To ensure this reliability, events cannot be timestamped through sole use of the computer's internal clock, as this is easily falsified and deviates naturally over time. The ANSSI first recommends synchronizing the clocks of IT equipment with several internal time sources that are coherent with each other, themselves synchronized with several reliable external sources.[34] Secondly, a logging system must be set up in accordance with applicable regulations and the recommendations of the CNIL insofar as the main objective of logging is to allow the person or the equipment causing an event to be identified directly or indirectly. Finally, logs must be signed and timestamped as soon as they are created so as to ensure their integrity.



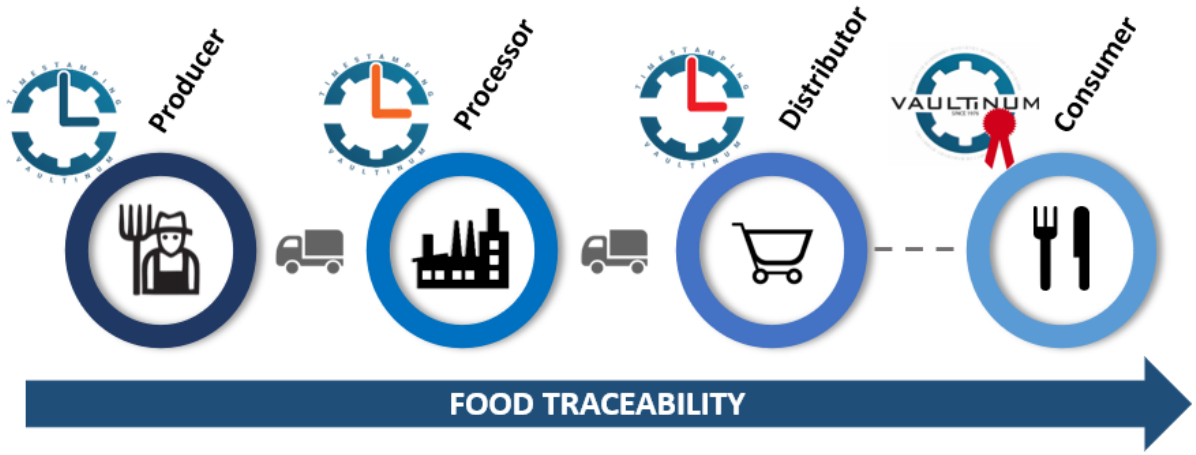
4.5 Supply chain

As a large-scale distributor, I would like to ensure the traceability and transparency of some of my products of animal origin. How can I do this?

Following a number of scandals that testified to a lack of supply chain transparency in the food industry, regulation no. 178/2002 of 28 January 2002 introduced a requirement for food traceability at all stages of production, processing and distribution[35] in order to identify sources of contamination more quickly.

[34] Agence nationale de la sécurité des systèmes d'information, *Note technique – Recommandations de sécurité pour la mise en œuvre d'un système de journalisation*, 2 décembre 2013.

[35] Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety, art. 18.



The same question arises with regard to environmental protection. Soon, food and product traceability will allow for the display of information on the environmental footprint of a product.

In terms of supply chain (agro-food, luxury goods, wine, pharmaceutical industry), electronic timestamping and, more generally, timestamping applied to "blockchain" technology (a chain of records allowing to keep track of a set of information, in a decentralized, transparent and secure way), has a real potential to ensure timestamping, traceability and control of the origin of a product.

At every stage of the supply chain (producer, processor, distributor), a certain amount of information (dates, origin) concerning a food product, from its manufacture to its sale, will be recorded in a timestamped blockchain register. Depending on the case, the recording on the register could be done either by means of human intervention such as a photograph of the items, or automatically, through the use of connected sensors.[36] Each actor in the supply chain can access the blockchain register to learn the identity of the person who first entered the information, the content of information itself (the integrity of which is guaranteed), and the date of registration of this information.

And yet, blockchain has its limits. Distributors and other importers need to protect their commercial networks and other trade secrets. The transparency of blockchain prevents this protection, but another solution exists. It consists of validation by a trusted third party by virtue of the presence of secure, timestamped register systems at each stage of the supply chain.

In practice, a leading European brand has already chosen blockchain timestamping for its chicken industry. Each actor in the supply chain can enter and timestamp traceability information which is of interest to them, and which will, for the most part, be communicated to the consumer by means of a QR Code[37].

Vaultinum provides support to its clients in setting up a timestamping system to date the events registered throughout the supply chain. Using the Vaultinum API, client or blockchain

[36] Etude réalisée par Blockchain Partner, *Supply Chain, Traçabilité & Blockchain*, 10 juillet 2017.
[37] Dalila BOUAZIZ, *Carrefour lance la première blockchain alimentaire d'Europe*, E-commerce mag, 6 mars 2018.

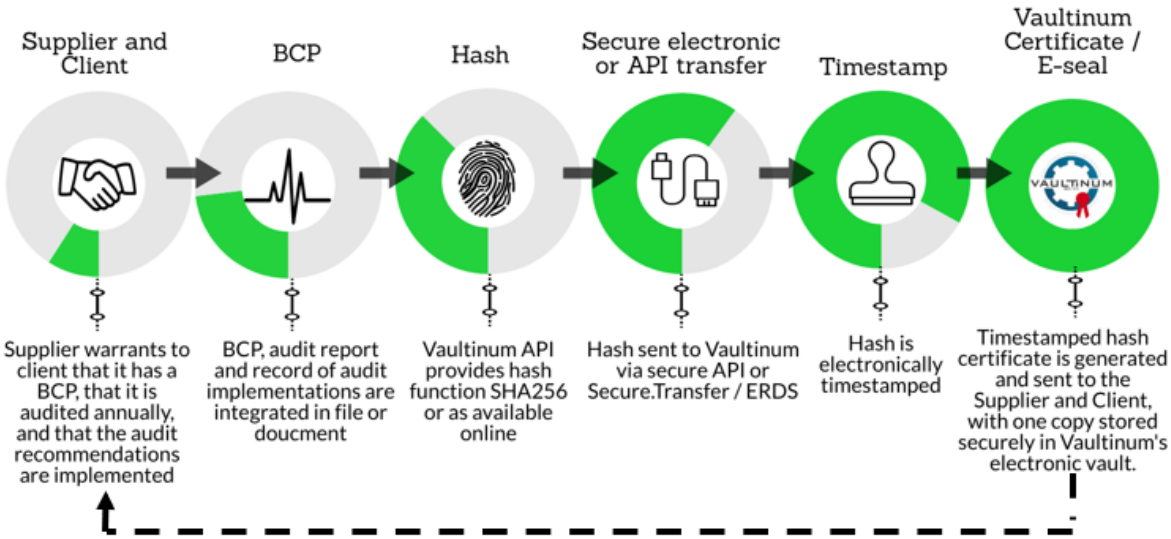
systems can interface with Vaultinum's timestamping solution and continuously and automatically timestamp thousands of events in a reliable, secure and adaptable manner.

4.6 Quality assurance and monitoring of document versions

To play it safe, my service provider has put in place a business continuity plan ("BCP") to manage force majeure or crisis situations. This BCP is essential for my business. It is updated every year. How can I be sure that the plan I have is the latest version and that it has not changed?

Business continuity plans (BCPs) have long been required by buyers of products and services. These plans are generally tested and updated annually. They are essential because they provide information on the measures taken to avoid service interruptions on the supplier's side, for example, in the event of unforeseeable events or natural disasters and, and in turn, on the buyer's side. As such, it is essential that tests and updates are timestamped and securely archived in order to maintain documentary evidence over time and ensure the legal protection of all parties concerned.

Vaultinum provides secure and reliable archiving and timestamping services.

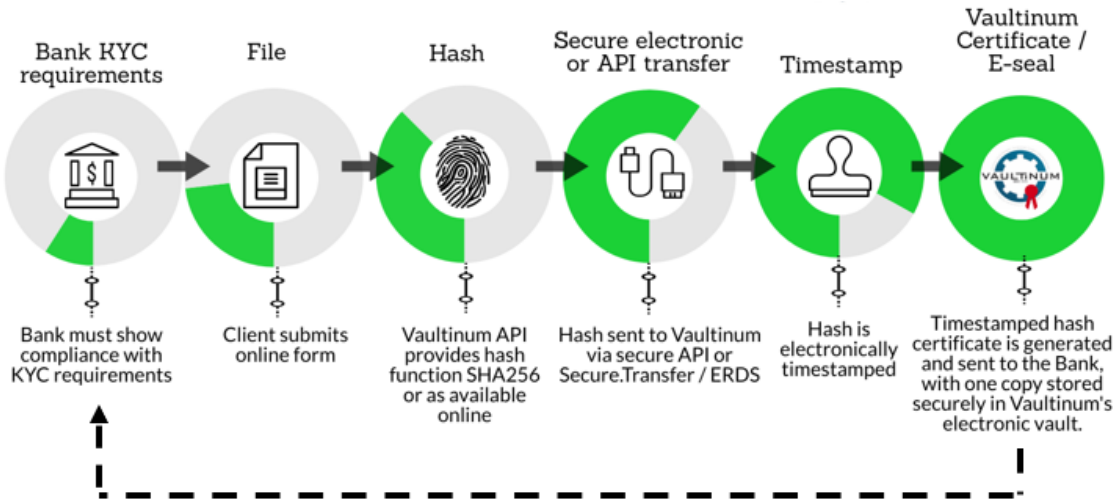


4.7 Banking and insurance

Data and information are often submitted online and are sometimes used to generate positions, offers or assessments. In order to avoid any dispute related to the content of the information submitted and its date of submission, and to guarantee that requests are dealt

with properly and within a given timeframe, content should be archived securely and with a timestamp token.

Vaultinum supports banks and insurance companies by offering them a turnkey solution for timestamping and secure archiving of online requests. This adaptable, reliable and secure solution enables the automation of certified timestamping and secure archiving, thanks to the Vaultinum API.



4.8 Invoicing

Invoicing has a number of consequences, particularly in terms of payment deadlines but also with regard to deadlines for taxes and other fees. How can I make sure that I can provide proof of electronic invoicing and the date it was issued/sent?

The digitization of invoicing processes promises significant efficiency gains and cost reductions. At the tax level, article L 102 B of the French Tax Procedure Code, amended by article 16 of the Amending Finance Law for 2016 allows taxpayers to digitize their paper invoices received and issued and to keep them in digitized format for the fiscal retention period of 6 years. The regulations specify that digitized invoices must meet two conditions; they must be secured to ensure their integrity, and they must be timestamped. Although the timestamp can be internal, a timestamp certified by a trusted third party or a qualified timestamp process is essential to avoid disputes, especially since the timestamping of invoices is also used to enforce payment deadlines and calculate late payment penalties.

Vaultinum has developed an API to which clients can connect to obtain an automated certified timestamp of each document with the additional possibility of secure archiving.