PRIORITY FOR EVERYONE

from

Ralf Schönmeyer *

Abstract

The author discusses a new practical approach for Statements of Priority – preceded by an overview of the current state of the art.

Scientists, inventors, authors, artists and other creators of works are familiar with the problem: distributing their work creates a risk that others replace or deny their authorship.

In Germany, copyright law applies at the moment of the creation of a work, but according to § 10 UrhG, the creator is given the benefit of the doubt – as long as the opposite is not proven and e.g. a lawsuit reveals evidence of work at a prior date.

As an example of the problem, a designer is appointed by a company to create a new logo. The company reviews the drafts but graciously declines. A minimal fee occurs. Later it emerges that the company is using a logo that has striking resemblance to one of the drafts of the designer. A lawsuit is conducted about creatorship, and damages for lost business are considered. The company may simply claim that the idea for the logo was already in existence, and their own design occurred independently of the designer. Without additional proof, one testimony stands against another and the designer is virtually left empty-handed.

Similar situations occur in other fields: e.g. when scientists prepare publications with new data or methods; when freelance journalists wish to submit texts; or when composers perform their newest song to a potential producer.

Accordingly, creators of copyrightable work all have an interest in documenting the time of creation before presentation to third parties. System-timestamps from documents or emails provide little protection, as they are easy to change.

The common procedure of sending a registered letter to oneself and keeping this letter unopened (containing specifications, and with a postal date stamp) does not constitute a complete chain of evidence. In doubtful cases, its authenticity can be questioned. The legal value of date stamps from electronic communication services – such as SMS, DE-Mail or E-Postbrief – is undetermined and long-term storage raises open issues.

One possibility is to deposit creation-documents at a notary. This is legally authoritative: the date of receipt is acknowledged and it constitutes reliable proof. But this involves high fees – typically between 50€ to 100€ per declaration of priority and subsequent archival. In the initial stages of development, few people are willing to accept such costs – especially when the long-term value of a work is unclear.

For some time, internet-based services [1] are available that digitally transfer relevant documentation to a notary. This offers a more attractive cost structure – with no postal charges and easier archival – but the costs can nevertheless remain prohibitively high for personal users. Many creations won't be protected in this way until later stages of development. Privacy is also potentially compromised by the transfer of documentation.

An alternative can be achieved by applying hash-based algorithms. A secure hash function will map a string of arbitrary size (e.g. the contents of a file) to a shorter string of fixed length. One can imagine this *hash value* as a unique digital fingerprint of the file. There are established standards for hash functions that are recognized as secure and which play an important role in cryptography – e.g. the widespread SHA-2 standard. With SHA-2, it's not realistically possible to create another file that exhibits the same hash value. If the contents of a file are changed, the associated fingerprint (the hash value) also changes. This is a mathematical certainty and many critical applications rely on this, e.g. for secure saving of passwords. An additional advantage is privacy: conclusions cannot be inferred from the hash-value about the contents or properties of the original data. Determining the identity of a file by SHA-2 hashes has greater certainty than determining the identity of a person by DNA test – routinely used in trials in spite of the known risk of procedural errors. Testing a SHA-2 value can be performed by independent experts, both repeatedly and retroactively.

When a SHA-2 hash value of a document is stored together with a reliable time statement, this constitutes a proof that the exact contents of this document have existed since that time. This can be used to confirm a disclosure. In a lawsuit, owners of the original document can reproduce the associated hash value and compare it with the archived version. If both are identical, the proof is valid.

A classic usage is to publish the hash value of a document in a printed newspaper. This establishes a commonly accepted date of publication, not realistically alterable thereafter – as newspapers are both reputable and widely distributed. It seems this method is rarely used – at least, newspapers usually don't have many insertions with strange texts (from a preliminary version of this text, a 256-bit SHA-2 hash-value of 64 characters looks in hexadecimal notation like: 7C6FE1BE2B68352C 5B923E96DF86DD9E 010788568B7B2892 232444EA8F71B02C3).

Internet-based services exist which provide similar credibility to a trusted time stamp. For frequent users, the time and money-costs of these services outweigh the costs of commissioning and archiving of newspaper insertions. Services like [2] certify the time-of-creation of a hash value. Aside from trusting the service provider, registration is required and prices depend on the amount and volume of documents to be protected.

However, for occasional users these costs still constitute a barrier.

Secure as a bank!

Safer, simpler and cheaper proofs of priority can be performed in this way:

1. Produce – with software of your choice – a secure hash value for the document: e.g. a SHA-2 value with 256 bits (SHA256).
2. Put this value into the subject field of an (online) bank transfer and pay an arbitrary amount of money (e.g. one cent) to another account – ideally at another bank.

The bank reliably archives the date of the transfer. Combined together with the text in the subject fields (which contain the hash value), there is evidence that the document existed at the instant of the transfer.

The benefits of this method are numerous: first, the costs are incomparably low. For many bank account packages, there is a flat-rate monthly fee, allowing unlimited bank transfers at no additional cost. This allows for regular protection of creations, even at early stages of development. With little effort this can be performed easily from your computer (e.g. using the author's software utility, freely-available here [3]).

As no dedicated implementation of the hash function is needed, there is no dependency on any particular software or manufacturer – in court, also. This method is generally compatible with current-accounts from all banks. No person can change the date or the text fields of a bank transfer belatedly. When the transfer has been cabled between two different banks, it is fully documented independently. The destination account may also belong to the sender, so no money is lost, and no third party can recognize the transaction.

The bank account statements constitute documents which archive the dates and hash values.

Banks must archive data about bank transfers for at least 10 years in Germany, and are obliged to hand out this information on request – helpful if an account statement is lost.

This method allows for high levels of proof. Third parties can verify a transfer directly with the banks where doubt arises.

Additionally, the authorization of a bank transfer in online banking – e.g. by a TAN system – constitutes a personal identification of the sender that is not easily established with other methods.

For creations of high-value, it's still advisable to employ a notary. Remember, that the worth of the archived hash values depends on the availability of the original documents. So reliable backups are important, but these should occur in any case.

For professional users, the online-integrated-service-solutions offer advantages, e.g. when time stamps are required very frequently.

However, circumstances aside, our method allows everybody to easily and cheaply create proofs of priority.

It also offers benefits in fields not involving copyright, when used to acknowledge possession or receipt of documents.

E.g. administrators can “sign” log files or backups to prove that no alterations have occurred after the documented date of the bank transfer.

Similarly, for other potential pieces of evidence – e.g. digital versions of documents, photographs, videos or audio files – it doesn’t harm to document their status at an early stage, which can be later verified as needed.

[1] http://www.priormart.com, http://www.notatus.de

[2] http://www.digistamp.com, http://www.surety.com

[3] http://www.schoenmeyer.de/prioprepare

*) This text is the translation of an article originally published in German here:
http://www.jurpc.de/aufsatz/20130111.htm