Journal of
Artificial Intelligence and Soft Computing Techniques

Review Article Open Access

The Problem of Loss of Validity of an Electronic Signature with a Certificate: Problems and Solutions

Andrey Shcherbakov[1,2*]

[1]Department of Cognitive Analytical and Neuro-Applied Technologies, Russian State Social University, 129226 Moscow, Russian Federation

[2]State University of Management, 109542 Moscow, Russian Federation

[*]**Corresponding Author:** Andrey Shcherbakov, Department of Cognitive Analytical and Neuro-Applied Technologies, Russian State Social University, 129226 Moscow, Russian Federation, E-mail: x509@ras.ru

Received Date: July 04, 2025 **Accepted Date:** July 16, 2025 **Published Date:** July 19, 2025

Citation: Andrey Shcherbakov (2025) The Problem of Loss of Validity of an Electronic Signature with a Certificate: Problems and Solutions. J Artif Intel Sost Comp Tech 2: 1-7

Abstract

The problem of the loss of validity of electronic signature certificates over time is considered and two ways of solving the problem are proposed - for a period of several years - a method of re-signing documents with a timestamp and for a period of 50-100 years, a method associated with the use of hashing, with a complete rejection of the use of certificates.

Keywords: Electronic Signature; Banking Sector; Hashing; Certificates; Loss of Signature

Introduction

Recently, practitioners of the use of electronic signatures, especially in the banking sector, often have problems with the loss of signature validity. It is worth paying attention to three scenarios in which this can happen.

1. There are cases when the owner of the signature refuses to sign the document, arguing that it was a hacker attack that led to the theft of the signature key. There is a law enforcement practice when the court sides with the owner of an electronic signature and the signed document is declared invalid. There are currently no effective measures that an organization or individual could take to counteract such a scenario, except for insurance of the designated risk.

2. If the electronic signature key is compromised, its owner must report this fact to the Certification Center (CC) that issued the electronic signature certificate. As a result of the request, the certificate corresponding to this electronic signature key is placed in the list of revoked certificates. Usually, the verification of the electronic signature key at the time of signing the document takes place with preliminary verification that the certificate is not on the revoked list. However, it takes some time for the compromised certificate to be placed on the revoked list, during which time the compromised electronic signature can be used to sign the document, after which the validity of the signed document can be challenged. The use of this method for fraudulent purposes is also documented in judicial practice, the investigation of such cases can take several years and the result is not predictable.

3. Upon expiration of the electronic signature certificate, the signature on all documents that are signed with this electronic signature becomes invalid (unsuitable for verifying the authenticity of the document in court). This is a strategic disadvantage of modern electronic signature and verification systems based on certificates. In short, an electronic signature is verified using a public key signed by a trusted management system, which is used, in turn, to verify the electronic signature under an incoming document. At the same time, electronic signature certificates have a limited validity period, usually one year. Certifying centers are not legally required to store and provide electronic signature key certificates after their expiration date. Accordingly, verification of the document's signature by a standard procedure will produce the result "The electronic signature key has expired", even if the signature was valid at the time of signing the document. Such a signature cannot be used in court to prove the authenticity of the document.

Here, for example, is what [1] writes about this:

“What to do if the electronic signature certificate expires

In order for an electronic signature to remain active, its holder must independently monitor the expiration date. We recommend that you apply for an extension two weeks before the certificate expires. If you do not meet the deadline, you will have to visit the Certification Center in person to confirm your identity.

Maximum validity period of an electronic signature certificate

Electronic signature certificates are usually valid for 15 and 12 months. The term may depend on the requirements of the certification center itself, and the request of the future owner. For example, the Federal Tax Service Management Center issues certificates strictly for 15 months. And the Center of Certification (CS) Contour is from 3 to 15 months old.

The validity of the electronic signature certificate may expire earlier. This may happen at the request of the owner, due to the closure of the certification center, or by court order."

In the article [2], the authors draw attention to a similar problem related to the long-term storage of digitally signed data.

Documents signed with an electronic signature, for example, in the banking sector, notary public and intellectual property protection, have significant expiration dates and storage. For example, the charter of an organization that serves to compile a credit dossier may not change for several years, after which it will be impossible to verify the electronic signature due to the expiration of the certificate. At the same time, the immutability and authorship of the document, fixed by the signature, will be valid. The same applies to digital wills and other patterns of transfer of rights through long retention periods.

The Issue of Certificate Expiration Date

A partial tactical solution to this problem is to sequentially place time stamps under the document after checking the electronic signature on the valid certificate (for example, every year). The timestamp is generated by an external trusted service and can also be verified using it, which makes this process objective with the participation of a third party. For signing with a timestamp, a hash function of the document is provided, according to which it is impossible to restore the content of the document, therefore, the risks of violating the confidentiality of documents in this case are excluded.

Accordingly, the organization must implement on its side a special verification service that will additionally sign all received and verified documents with the customer's electronic signature in a specialized external trusted service that will verify that the customer's electronic signature on the document was made no later than the current date when the customer's signature is still guaranteed valid. At the same time, such a certifying signature of an external trusted service containing a timestamp is also limited by the validity period of its electronic signature certificate. Therefore, such a service must monitor the validity period of all such certificates, and timely re-sign the expiring signature of an external management center with a new signature in the same (or in another) external management center, at least once a year. In this way, an electronic signature chain will be created, in which each subsequent electronic signature certifies the previous one, and the most recent electronic signature always remains fresh and verifiable. As a result, the existence of the customer's electronic signature at a certain point in time in the past can be proven on any date during the time period during which we have a chain of re-signing.

The procedure should be fine-tuned and work smoothly for all legally significant documents with an electronic signature throughout their entire period of demand and archival storage. We currently have no information about the use of this kind of evidence in court or about the current practice of making decisions based on them, but it is obvious that this provides an additional objective argument in court in favor of the authenticity of the document.

The Situation of Long-Term Document Storage

It seems that cryptographers who deal with electronic signatures live only in the present moment and the desire to sell their crafts that do not always work well.

In general, it can be stated that the electronic signature system for long-term stored documents currently does not fully justify itself simply because the task statement is different.

The situation becomes even more complicated if we consider documents of long-term storage, for example, a will or digital images of some persons who have been deposited now, and will be "avatarized" (revived) in 50-100 years.

In this case, it is proposed to completely abandon the use of certificates and build a rights verification algorithm based on hash functions.

Hash functions [3] have a number of requirements that can be divided into general and cryptographic ones. - Common requirements include determinism, fast computability, and collision tolerance. Cryptographic hash functions, in addition to the general ones, must have the properties of irreversibility (resistance to preimage and second preimage) and avalanche effect.

General Requirements

Determinism: For the same input value, the hash function must always produce the same hash code.

Speed of calculation: Hash function calculation should be fast and efficient, regardless of the size of the input data.

Collision resistance: It should be extremely difficult or practically impossible to find two different input values that lead to the same hash value.

Cryptographic Requirements

Irreversibility: Resistance to finding a prototype-

: It is not possible to calculate the input value from its hash value.

Resistance to finding a second prototype: It is impossible to find another input value that has the same hash as this input value.

Avalanche effect: A small change in the input data should result in a significant change in the hash value.

Fixed length of output data: Input data of any size must produce a fixed-length hash value.

In general, a good hash function should be fast, collision-resistant, and irreversible, as well as have an avalanche effect.

The task is for the owner of some information in a universal format, for example, the text T in human-readable form or the digital sequence M in machine-readable (computer-readable) format, to prove some of his rights to information stored for a long time, when there are no legal entities, private unknown firms that owned these legal entities, various "state-owned corporations" that they for some reason, this was allowed, there are simply no electronic signature verification algorithms anymore, either, not to mention certificates, which have also sunk into the past for complete commercial uselessness.

Long-term Digital Identifiers

Let's introduce a few terms

A project participant (PP) is a natural or legal person who has given documentary consent to participate in a long–term project, for example, to create a digital image of a person [4] or a person who has left a long-term will.

The main identifier of the PP (MI PP) is a digital sequence of the recommended length that uniquely describes the PP and is associated with it, while according to the MI PP it should be impossible to establish the identity and personal data of the PP.

The payment identifier of the PP (PI PP) is a digital sequence of the recommended length that uniquely describes the PP in terms of financial transactions for servicing operations with the Central Bank. According to the PI PP, it should be impossible to establish the identity of the PP and the MI PP.

Let's assume that we need to get an MI PP and a PI PP for some array of M without using certificates, and in general, it's better without an electronic signature.

Let's say that we have a hash function H. Let's also assume that this hash function is algorithmically described, for example, in the form of a flowchart, mathematical formula, text, code fragment in a universally understood programming language and a test case is connected to it. A test is an arbitrary sequence for which the result of its calculation is known:

ht = H (Test)

Without limiting generality, we also assume the existence of solid human-readable media that ensure the immutability of the Ti text written on them and conversion algorithms that have the ht test result and a sufficiently compact recording described above.

Let the PP form a unique text Ti, where “i" is the conditional number of the PP. This text can describe the PP, for example, contain his name, pseudonym, date of birth, number in government or corporate accounting systems, and so on, and in any format.

Next, using H, the PP generates hi = H(Ti).

Let's also assume the existence of a subject (organization) "Library" or "Notary", which stores important information for the PP, for example, its digital image or Mi testament.

It calculates hmi = H(Mi) and passes it to the PP.

The PP fixes it on the media (possibly on the same one where he recorded Ti). After that, he transfers the previously calculated hi in some way to the librarian or notary, who stores Ii and hi for the necessary time.

The User's Rights are Checked as Follows

He presents the Ti on a medium (the properties of the medium do not allow you to change the Ti, however, if you change it, the Torah does not match the one that the notary or librarian has).

Next, the hash function H itself is checked – the test is calculated, he = H(Test).

If he is equal to ht, then this is the same hash function that was used at the beginning of fixing the rights of the PP.

Next, the PP demonstrates the calculation of hi on a verified hash function for Ti, and the notary checks whether the result matches the one he has stored.

Next, the notary demonstrates that the hesh of M i matches the one available to the notary.

Thus, the parties are convinced of their rights and perform certain actions based on the checks made, for example, they "revive" the Mi.

In the current activity, hi can be used to generate a payment identifier, hpi=H(hi), which will not allow you to identify hi and Ti, but nevertheless, use it to perform unique payment transactions on behalf of Ti.

The algorithm for fixing and verifying rights is briefly shown in Table 1.

Table 1

Fixing rights		
Participant (user, client)		Custodian (notary public, library)
The participants and the guardian have a test ht=H(Test)		
Ti is the client's description (identifier, IDs). There can be several client IDs		Mi – testament or digital image (avatar)
hi = H(Ti).	-------------------------------->	
	<--------------------------------	hmi = H(Mi)
Ti, Mi, Hmi and hi are stored for the required time		
It's been 100 years		
Rights verification		
The parties calculate the he=H(Test) test.		
	If he matches ht, then both sides use a non-replaceable hash function.	
hi = H(Ti)	--------------hi, Ti -------------->	The keeper checks for a match hi with the value he has
The participant checks if the hmi matches the value he has	<------------Mi, hmi------------	hmi = H(Mi)
If there is a coincidence, the parties have confirmed their rights and proceed to legal action.		

From the point of view of technical applicability and convenience, you can choose any of the well-studied hash functions with excellent cryptographic properties: GOST P 34.11-94, BelT, BLAKE, Blue Midnight Wish, CubeHash, ECHO, Edonkey2k, FSB, FugueGrøstl, HAVAL, Hamsi, JH, Kupyna, LM hash, Luffa, MASH-1, MD2, MD4, MD5, MD6, NHash, RIPEMD-128, RIPEMD-160, RIPEMD-256, RIPEMD-320, SHA-1, SHA-2, SHA-3, (Keccak), SHA-256, SHABAL, SHAvite-3, SIMD, SWIFFT, Skein, Snefru, Tiger, Whirlpool.

The selection criterion may also be the compact recording of the hashing algorithm and the ease of programming it to calculate a test case.

Legal Aspects of Using Hash Functions

The use of hash functions in the legal field, especially in the context of digital technologies, raises a number of issues related to legal recognition and use. The main legal aspects relate to the evidentiary power of hash functions, their role in ensuring data integrity and security, as well as possible risks and vulnerabilities.

The main legal aspects of using hash functions.

1. The evidentiary power of hash functions

In court, hash functions can be used to verify the integrity of electronic documents, files, and other data. If the hash value of the document matches the one that was recorded earlier, this can serve as proof that the document has not been modified.

To recognize the evidentiary value of hash functions, a number of factors must be considered, such as the reliability of the hash function used, compliance with the protocol of its application, and the availability of independent confirmation of the results.

For example, in Russia, there is GOST R 34.11-2012, which sets requirements for cryptographic hash functions used in the field of information technology.

2. Password Security and Storage

Hash functions are widely used for secure password storage. Instead of storing passwords in the clear, they are hashed, which significantly increases the security of accounts.

It is necessary to use hacking-resistant hash functions and implement them correctly to avoid the risks of password leaks and unauthorized access to accounts.

3. Data Integrity Check

Hash functions allow you to check whether data has been changed during transmission or storage. This is especially important for mission-critical data such as legal documents, financial transactions, etc.

If the hash value of the document received after its transmission or storage matches the original hash value, this confirms that the data has not been modified.

4. Digital Signatures

Hash functions are an integral part of the process of creating and verifying digital signatures. A digital signature is created based on the hash value of the document and the secret key belonging to the signatory.

To ensure the legal significance of a digital signature, it is necessary to use certified cryptographic information protection tools and comply with relevant regulatory requirements.

5. Risks and Vulnerabilities

It is important to understand that hash functions are not completely invulnerable. There are attacks aimed at finding collisions (different input data giving the same hash) or at restoring the original data from the hash value (if the hash function is not sufficiently stable).

It is necessary to use reliable hash functions and apply them correctly to minimize risks.

6. International Standards and Legislation

Different countries have their own standards and legislation governing the use of hash functions in a digital environment.

It is necessary to take these standards and legislation into account when applying hash functions in the legal field.

Conclusion

In conclusion, hash functions play an important role in ensuring data security and integrity in the digital environment, and their legal aspects require careful consideration and compliance with relevant norms and standards.

The proposed method allows you to verify that the owners of information have certain rights without using an electronic signature and certificates.

References

1. https://ca.kontur.ru/articles/52807-srok_dejstviya_elektronnoj_podpisi

2. Jennifer Shivers, Paul G. Biondich (2019) Cross-border Health Information Exchange to Achieve World Health Outcomes. Center for Biomedical Informatics, Regenstrief Institute, Inc., Indianapolis, IN, USA, Global Health Informatics, Regenstrief Institute, Inc., Indianapolis, IN, USA. 20: 171-213.

3. Bruce Schneier (2002) Applied cryptography. Protocols, algorithms, source texts in C. Moscow: Triumph, ISBN 5-89392-055-4.

4. Digital image. The "Eternity" platform. https://birch-league.com/