1.08 Objavljen znanstveni prispevek na konferenci
1.08 Published Scientific Conference Contribution

*Hrvoje STANČIĆ**

LONG-TERM PRESERVATION OF DIGITAL SIGNATURES

Abstract:

Digitally born documents are increasingly being signed by digital signatures. Once becoming records, they need to be preserved – in some cases for several years while in other cases permanently. In essence, what should be preserved besides digital records themselves, is their trustworthiness. This may be a problem because digital records might be converted to new formats, migrated to new media, emulated or virtualised in new environments due to the technological obsolescence. Authenticity, in particular, relies on the possibility to check the validity of the digital signature. However, digital signatures expire after a certain period. The author investigates the possibilities of long-term preservation of digitally signed records in the ever-changing IT environment.

Key words:

digital records, digital signatures, digital certificates, long-term preservation, archival science

Izvleček:

Dolgoročno varovanje digitalnih podpisov

Izvorne digitalne dokumente vedno pogosteje podpisujemo z digitalnimi podpisi. Ko tako postanejo del zapisa, jih je potrebno ohraniti – običajno nekaj let, v nekaterih primerih pa tudi trajno. Poleg samega digitalega zapisa je nujno ohraniti tudi njegovo verodostojnost. To lahko predstavlja problem, saj so lahko digitalni zapisi pretvorjeni v druge oblike, preneseni na nove medije ali virtualizirani v novih okoljih zaradi zastaranja tehnologije. Avtentičnost dokumenta še posebej sloni na možnosti preverbeveljavnosti digitalnega podpisa. Le-ta pa po določenem obdobju preneha. Avtor raziskuje možnosti dolgoročnega varovanja digitalno podpisanih zapisov v vselej spreminjajočem se IT-okolju.

Ključne besede:

digitalni zapisi, digitalni podpisi, digitalna potrdila, dolgoročna hramba, arhivska znanost

1 INTRODUCTION

Digital communication has become a standard way of communication today. One would imagine that all digitally born documents and records are being preserved in the digital form, but this is not the case. Many of them are being printed out, signed and preserved in the paper form as evidence of a course of business or a transaction being made. Presence of signature, accompanied with other forms of authentication, e.g. seals, differentiates originals from copies. It is always possible to differentiate the two in the analogue world. There is usually a fixed number of originals, one or several in case of, e.g. agreements, and the authenticated copies may be made, e.g. by a notary, using the originals. Also, the signature that the author applies to many different documents should be (ideally) the same in order to differentiate between the author's signature and the forged signatures. The originality of a signature may be subject of a forensic analysis and determined as authentic on the basis of graphological characteristics. All this

* *Hrvoje Stančić, Ph. D., associate professor, Department of Information and Communication Sciences, Faculty of Humanities and Social Sciences, Ivana Lučića 3, Zagreb, Croatia, contact: hstancic@ffzg.hr.*

fundamentally changes once the digital signatures are introduced. First of all, as it will be presented later on, every digital signature from the same author is different from one another. Then, there may be infinite number of originals since making a digital copy of a digital original may maintain every characteristic of the original and may function as an original. Therefore, we cannot apply the concept of original from the analogue to the digital world. We have to change the paradigm regarding the originality since the authenticity of the digital signature cannot be verified without a third party, as it will also be argued later on. Considering all this, it is important that archivists understand the mechanisms behind digital signatures in order to be able to verify authenticity, integrity and non-repudiation of a message, document or a record and to be able to reach an informative decision in the context of (long-term) digital preservation.

2 DIGITAL SIGNATURES

What primarily differentiates analogue from digital signatures is that the digital signature will be different for every document an author signs. The concept behind digital signatures lies on the concept of Public Key Infrastructure (PKI) using which the author generates a pair of two keys – private key and public key. The private key never leaves the author and the public key is made publically available.

There are two types of digital signatures – *basic* and *advanced*. Stančić, Rajh and Brzica (2015, p. 213) explain that »the EC Directive 1999/93 on a Community Framework for Electronic Signatures states that an electronic signature needs to meet the following requirements to become an advanced electronic signature:

a) it is uniquely linked to the signatory,

b) it is capable of identifying the signatory,

c) it is created using means that the signatory can maintain under his sole control,

d) it is linked to the data to which it relates in such a manner that any subsequent change of the data are detectable«.

Further, Brzica, Herceg and Stančić (2013) describe that digital signatures can be realised in several formats – XML Digital Signature (XMLDSig), XML Advanced Electronic Signature (XAdES) (which can be realised as XAdES-BES, XAdES-T, XAdES-C, XAdES-X, XAdES-X-L, and XAdES-A), Cryptographic Message Syntax Advanced Electronic Signature (CAdES), and PDF Advanced Electronic Signature (PAdES).

When the author wants to digitally sign a document, he applies his private key to the document and sends it to the recipient. The recipient, by applying the author's public key to the received document, can verify if the author has signed the document. The result of the verification is a simple »Yes« or »No« (i.e. the author either did or did not sign the document). If the document has been changed, the application of the author's public key to the changed document would result with refutation. The important thing is that it is mathematically impossible to calculate private key from the public key.

The author can also calculate the so-called *document digest* by applying the hash algorithm to the document (e.g. using MD5 method). The result is a 128-bit number,[1] which is unique for every document. If a document changes, its digest would change too. Friedl (2005) argues that the creation of the document digest is *collision resistant*, i.e. that there are no two different documents for which the same digest would be calculated. Also, it is impossible to reverse the operation and get the contents of the document by knowing the document digest.

For example, hash value calculated from the abstract of this paper using MD5 method is: »b998ff7b2695ad3d22233ed226fdfbe3«. If only one letter is changed, e.g. if the initial word »Digitally« is changed to »digitally«, the MD5 method would generate a substantially different hash value, e.g.: »72fe719ffbf0cf7d5e8784 dda3e87bbc«, for the whole abstract.

When the author wants to digitally sign a document, he applies his private key to the document digest and sends it to the recipient. The recipient recalculates the document digest and by applying the author's public key to the document digest, verifies if the author has signed the document. This is a faster procedure with the same effect since the signature is either confirmed or refuted by checking against the document digest and not the whole document, which might be of considerable length.

The only thing we are still not sure is who is the real person standing behind the digital signature. There are numerous web services offering the creation of a combination of public and private keys and anyone can claim to be anyone else if (s)he wants it. Therefore, we need digital certificates.

3 DIGITAL CERTIFICATES

If we want to be sure that the author behind a digital signature is indeed that person and not someone else impersonating the author, we need a trusted third party called *certification authority*. Boettcher and Powell (2002) compare digital certificates to virtual ID cards issued by a trusted authority and explain that »a PKI includes organizations called certification authorities (CAs) that issue, manage, and revoke digital certificates. (...) A CA might create a separate registration authority (RA) to handle the task of identifying individuals who apply for certificates«. Google Chrome help section explains that »public key certificate, usually just called a certificate, is a digitally signed statement that binds the value of a public key to the identity of the person, device, or service that holds the corresponding private key«. Microsoft (2005) further clarifies that »because the certificate matches a public key to a particular individual, and that certificate's authenticity is guaranteed by the issuer, the digital certificate provides a solution to the problem of how to find a user's public key and know that it is valid. These problems are solved by a user obtaining another user's public key from the digital certificate. The user knows it is valid because a trusted certification authority has issued the certificate. In addition, digital certificates rely on public key cryptography for their own authentication. When a digital certificate is issued, the issuing certification authority signs the certificate with its own private key. To validate the authenticity of a digital certificate, a user can obtain that certification authority's public key

[1] *MD5 (Message Digest) produces 128-bit hash value, SHA-1 (Secure Hash Algorithm) produces 160-bit and the more advanced SHA-2 produces 224, 256, 384 or 512-bit hash value.*

and use it against the certificate to determine if it was signed by the certification authority.«

Picture 1: Example of a valid certificate

Picture 2: Example of an expired certificate

Microsoft Windows 7 help section explains that the »path validation involves processing public key certificates and their issuer certificates in a hierarchical fashion until the certification path terminates at a trusted, self-signed certificate. Typically, this is a root CA certificate. If there is a problem with one of the certificates in the path, or if it cannot find a certificate, the certification path is considered a non-trusted certification path. A typical certification path includes a root certificate and one or more intermediate certificates.«

Picture 3: Example of a certification path

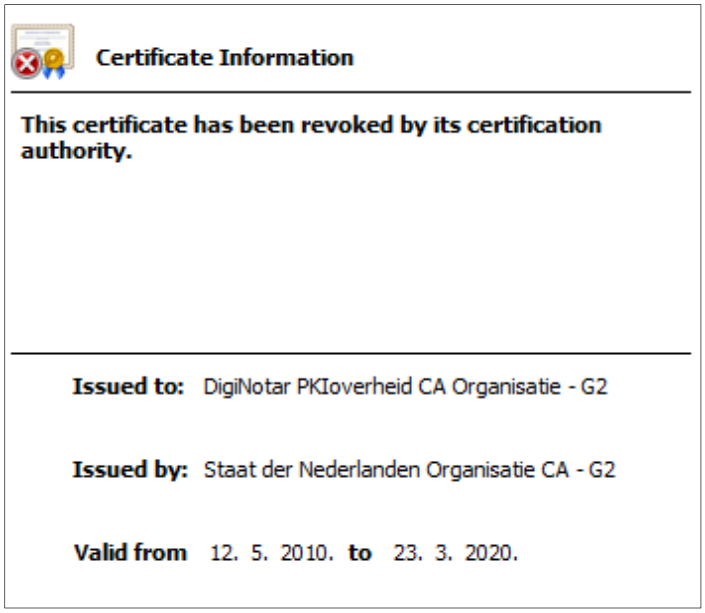
Boettcher and Powell (2002) differentiate between four types of certificates – root or authority certificates, institutional authority certificates, client certificates and web server certificates. Certificates that are commonly used today are conformant with the X.509 v3 certificate standard and may typically, according to the Chrome help section, contain the following information:

- the subject's public key value,
- the subject's identifier information, such as the name and e-mail address,
- the validity period (the length of time that the certificate is considered valid),
- issuer identifier information, and
- the digital signature of the issuer, which attests to the validity of the binding between the subject's public key and the subject's identifier information.

However, Brzica, Herceg and Stančić (2013, p. 149) point out that the »Directive 1999/93/EC allows issuing of the so called *qualified certificate* which is based on the RFC 3039 standard and implements the concept of non-repudiation« and enumerate 10 elements that a qualified certificate must include.

Digital certificates may be valid or may, for a particular reason, be revoked. The *certificate revocation list* (CRL), according to TechTarget (2007), is »a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue, and the entities that issued them, are also included. (...) The main limitation of CRL is the fact that updates must be frequently downloaded to keep the list current. Online Certificate Status Protocol (OCSP) overcomes this limitation by checking certificate status in real time.« In that context Brzica, Herceg and Stančić (2013, pp. 150–151) explain that »non-repudiation is a characteristic of a record that prevents any signatory to deny the action taken or the content of a record. In the Croatian legislation non-repudiation is associated with the advanced digital signature which is based upon qualified certificate. For a record to achieve and preserve characteristic of non-repudiation it is necessary to ensure:

1. digital identity of signatories,
2. real-time revocation of digital signature rights,
3. time-stamping of digital signatures after checking the list of revoked certificates, which ensures the validity of electronic signature at the time of signing, and
4. secure long-term preservation.«



Picture 4: Example of a revoked certificate

Modern archivists should understand the concepts explained here because digitally signed records are being ingested into the digital archives and that may prove to be a challenging task in the context of (long-term) preservation. This will be explained in detail in the following discussion.

4 LONG-TERM PRESERVATION

(Advanced) digital signatures and (qualified) digital certificates are being increasingly added to or associated with digitally-born documents and records. Further on, such records are being submitted for ingest into the digital archives[2]. Digital archivists should decide what to do with them, having in mind that the digital signatures, from the archival point of view, have a short validity period and that the associated digital signatures may be revoked at any time. All this adds uncertainty to the archival process and impedes the possibility to verify authenticity, integrity and non-repudiation of a record after a certain period of time. To make things even more challenging, not only that digital archives are facing the dilemma whether to preserve digitally signed records or not, but they themselves are using digital signatures. PREMIS (2015, p. 259–260) explains that »the preservation repositories use digital signatures in three main ways:

1. *for submission to the repository*, an Agent (author or submitter) might sign an object to assert that it truly is the author or submitter;
2. *for dissemination from the repository*, the repository may sign an object to assert that it truly is the source of the dissemination;
3. *for archival storage*, a repository may want to archive signed objects so that it will be possible to confirm the origin and integrity of the data.

[2] *In this paper the terms »digital archive« and »digital/preservation repository« will be used with the same meaning.*

The first and second usages are common today as digital signatures are used in the transmission of business documents and other data. Typically, validation takes place shortly after signing and there is no need to preserve the signature itself over time. In the first case the repository may record the act of validation as an event, and save related information needed to demonstrate provenance in the event detail. In the second case the repository might also record the signing as an event but the use of the signature is the responsibility of the receiver. Only in the third case, where digital signatures are used by the repository as a tool to confirm the authenticity of its stored digital objects over time, must the signature itself and the information needed to validate the signature be preserved.«

According to Blanchette (2006, p. 14), from the point of view of archives, there are three possible solutions:

1. »*Preserve the digital signatures:* This solution supposes the deployment of considerable means to preserve the necessary mechanisms for validating the signatures, and does not address the need to simultaneously preserve the intelligibility of documents;
2. *Eliminate the signatures:* This option requires the least adaptation from archival institution, but impoverishes the description of the document, as it eliminates the signature as one technical element used to ensure the authenticity of the documents;
3. *Record the trace of the signatures as metadata:* This solution requires little technical means, and records both the existence of the signature and the result of its verification. However, digital signatures lose their special status as the primary form of evidence from which to infer the authenticity of the document.«

In order to preserve digital signatures along with the records, the archives should have the possibility to validate the signature at any given moment in the future. Due to the fact that digital signatures and associated certificates are valid only for a certain period of time and that the certificates might be revoked, as it was discussed before, this option seems rather unlikely to function at the long run unless certain preconditions are being met. Dumortier and Van den Eynde (2002) argue that »the only effective solution (in their view) for the problem of signature durability, is the archival of the original binary representation of the document. This solution was proposed by the European Electronic Signature Standardization Initiative (EESSI) in the study report *Trusted Archival Services* (TAS). A TAS must guarantee that it will still be possible to validate archived document years after the initial archival date, even if the applications that have been used at signature creation time are no longer in use. In other words, the TAS should maintain a set of applications (viewers as well as signature validation applications) together with the corresponding platforms (hardware, operating systems) or at least an emulator of such applications and/or environment in order to guarantee that the signature of the document can still be validated years later.« It is clear that this option would require a lot of technical skills and expertise from the archives, not to mention the financial implications.

The second option is technically the least challenging in the context of long-term preservation but it is actually not an option for archiving of the records that need to be preserved as authentic.

Therefore, for the long-term preservation of authentic digitally signed records, the third option is the most realistic one. Results of the InterPARES project recommend to organize a digital archives in a way to check the validity of the digital signatures at the ingest phase, to add the validation information to the records' metadata, and to preserve the records without addressing the digital signature's validity further. Thus, the issue of trust is shifted from the (digitally signed) record to the archives preserving digital records and the associated (validity) metadata. Gilliland-Swetland confirms this in Blanchette (2006, p. 14) by stating that »the findings of InterPARES indicate that integrity assurance and continuing accessibility are the key outputs of the archival recordkeeping function and that these are primarily assured through procedural and descriptive metadata. (...) Archival metadata must support the continued authenticity of records by describing the records as they were received from the records' creators and thoroughly documenting the entire process of preservation.«

5 CONCLUSION

The issue of long-term preservation of digitally signed documents and records is a relevant issue for the archival science and practice. On the one hand, they facilitate business, and digital transactions and activities could be made trustworthy and secure. On the other hand, trust in digital signatures depends on the information infrastructure and the hierarchy of interconnected certificates. Also, the validity of digital signatures and certificates is limited in time and this validity may be revoked at any given moment. Therefore, a level of uncertainty is always present and, as Ølnes and Seip argue in Foscarini (2008, p. 46) »the long-term storage of digitally signed documents cannot be relied upon for more than ten years«. This is because the signing methods that are secure at a certain point in time will become unsecure (within cca. 10 years) due to the advancements in the computing power that are still following the Moore's principle. That is precisely the motivation behind the transition from the (nowadays) less secure SHA-1 to the more advanced SHA-2.

A separate set of problems are connected with the digital preservation methods – conversion from older file formats to newer, migration from older media to newer, emulation, virtualization etc. Those procedures are necessary in the context of long-term preservation in order for digital records to stay readable and accessible. However, each of those procedures may substantially influence the authenticity, integrity, reliability, usability, and non-repudiation of the records. Thus, Groven (2010) points out, the validity information added to the metadata »becomes the primary evidence when, eventually, the bit integrity is broken and cryptographic tools are no longer valid after a transformation. For this reason verification and validation of digitally signed material is also very important to provide evidence of prior validity of digital signatures«.

To conclude, it seems that the most important thing in the context of this research is that the authentic digital records with still valid and verifiable digital signatures and associated certificates are submitted for ingest in a digital archives. From that point on, the digital archives should add the signature verification data to the records' metadata and preserve it for the long-term. In that case, the long-term preservation of digital signatures is not necessary as long as the validity information is preserved in the metadata. From that point on, users should trust digital archives for providing the information on the records' authenticity, not the records' themselves, because the digital archives should make sure that the digital

records are kept in a trusted archival environment and that no either unauthorised or authorised (preservation) procedure has influenced the aspect of trustworthiness[3] of the records.

Nevertheless, there are situations where the records are being kept in the live systems, or simply stored for quite some time before submitted for archiving. It might be that the digital signatures and the associated certificates are already expired at that moment and, as suggested in the earlier discussion, the archives could either ingest them without the authenticity information added to the metadata or refuse to ingest them. This could pose a problem if the law requires the records to be preserved and if the archives rejects them due to the non-validity of the digital signatures. Therefore, it would be a challenge to further investigate the possibilities of prolonging the period of validity of digital signatures.

6 FUTURE RESEARCH

The author will, along with other partners and as part of the recently initiated research topic at the InterPARES Trust project[4], investigate the possibilities of revalidation of the expired digital signatures, periodical re-signing of digital records, addition of timestamps, injection of additional (timestamped) proof of existence, etc.

RESOURCES

- Blanchette, J.-F. (2006). The digital signature dilemma. *Annales des Télécommunications, 61 (7-8)*, pp. 908–923. Accessed 6 January 2016 from: http://polaris.gseis.ucla.edu/blanchette/papers/annals.pdf.
- Boettcher, J. V. and Powell, A. (2002). *Digital Certificates*. CREN. Accessed 5 January 2016 from: http://www.cren.net/crenca/docs/syllabus.pdf.
- Brzica, H., Herceg, B. and Stančić, H. (2013). Long-term Preservation of Validity of Electronically Signed Records. A. Gilliland et al. (eds.), *Information Governance: Proceedings of the INFuture2013 in Zagreb 6-8 November 2013* (pp. 147–158). Zagreb: Department of Information and Communication Sciences, Faculty of Humanities and Social Sciences, University of Zagreb, URL: http://infoz.ffzg.hr/INFuture/2013/papers/INFuture2013.pdf.
- *Data Dictionary for Preservation Metadata: PREMIS version 3.0*. Accessed 3 January 2016 from: http://www.loc.gov/standards/premis/v3/premis-3-0-final.pdf.
- Dumortier, J. and Van den Eynde, S. (2002). Electronic Signatures and Trusted Archival Services. Proceedings of the DLM Forum: Access and preservation of electronic information: best practices and solutions Barcelona 6-8 May 2002 (pp. 520-524). Luxembourg: Office for Official Publications of the European Communities. Accessed 15 March 2015 from: http://www.expertisecentrumdavid.be/davidproject/teksten/DAVIDbijdragen/Tas.pdf.
- Foscarini, F. (2008). Cultures of Trust: Legal, Technical and Archival Perspectives on the Use of Digital Signature Technologies. Hegering, H.-G. et al (Eds). *INFORMATIK 2008 Beherrschbare Systeme - dank Informatik Band 1*, pp. 37–47. Bonn: Gesellschaft für Informatik. Accessed 7 January 2016 from: http://subs.emis.de/LNI/Proceedings/Proceedings133/gi-proc-133-007.pdf.
- Friedl, S. (2005). *An Illustrated Guide to Cryptographic Hashes*. Accessed 5 January 2016 from: http://www.unixwiz.net/techtips/iguide-crypto-hashes.html.

[3] *The concept of records' trustworthiness refers to authenticity, reliability, accuracy, integrity and usability of records.*

[4] *InterPARES Trust project, http://interparestrust.org.*

- Google Chrome help. *Certificates Overview*.
- Groven, A.-K. (2010). *Trust Strategies in Longterm Management and Preservation of Digital Records. A Deliverable to the LongRec Research Project*. Norsk Regnesentral. Accessed 18 December 2015 from: http://publications.nr.no/directdownload/publications.nr.no/5457/Groven_-_Trust_Strategies_in_Longterm_Management_and_Preser.pdf.
- Microsoft (2005). *Understanding Digital Certificates*. Accessed 5 January 2016 from: https://technet.microsoft.com/en-us/library/bb123848(v=exchg.65).aspx.
- Microsoft Windows 7 help. *Certification Path*.
- Stančić, H., Rajh, H. and Brzica, H. (2015). Archival Cloud Services: Portability, Continuity, and Sustainability Aspects of Long-term Preservation of Electronically Signed Records. *Canadian Journal of Information and Library Science, 39 (2)*, pp. 210–227. Toronto: University of Toronto Press.
- TechTarget (2007). *Certificate Revocation List (CRL) definition*. Accessed 5 January 2016 from: http://searchsecurity.techtarget.com/definition/Certificate-Revocation-List.

POVZETEK

*Hrvoje STANČIĆ**

DOLGOROČNO VAROVANJE DIGITALNIH PODPISOV

Digitalna komunikacija je danes postala standarden način komuniciranja. Prisotnost podpisa in drugih oblik avtentičnosti, kot so npr. žigi, je razlikovala originale od kopij. Nasprotno od analognih podpisov pa se vsi digitalni podpisi istega avtorja med sabo razlikujejo. Prav tako lahko obstaja neskončno število digitalnih originalov, saj digitalna kopija digitalnega originala ohrani vse značilnosti originala in lahko kot taka tudi nastopa.

Koncept digitalnih podpisov sloni na konceptu infrastrukture javnih ključev (Public Key Infrastructure - PKI). Avtor generira dva ključa – zasebnega in javnega. Zasebnega ima vedno pri sebi, javni pa je dostopen javnosti. Obstajata tudi dva tipa digitalnih podpisov – osnovni in napredni, izražena pa sta lahko v mnogih formatih (XMLDSig, XAdES, CAdES, PAdES). Če želimo biti prepričani, da za digitalnim podpisom stoji pravi avtor in ne nekdo, ki se zanj izdaja, potrebujemo še zaupanja vredno tretjo osebo, tj. overitelja, ki izdaja, upravlja in preklicuje digitalna potrdila. Potrdilo je digitalno podpisana izjava, ki povezuje vrednost javnega ključa z identiteto osebe, naprave ali storitve, ki je lastnik pripadajočega zasebnega ključa. Kvalificirano potrdilo prinaša tudi koncept nezatajljivosti. Digitalna potrdila so lahko veljavna ali preklicana in se tako znajdejo na seznamu preklicanih potrdil.

Za arhivsko znanost in prakso je poznavanje problema pomembno, saj se digitalno podpisani zapisi že zajemajo v digitalne arhive, to pa lahko pomeni precejšen izziv v kontekstu dolgoročnega varovanja. Arhivist se mora odločiti, kaj narediti z njimi, in hkrati razmišljati o tem, da imajo digitalni podpisi z arhivskega vidika kratek rok veljavnosti in so lahko kadarkoli preklicani. Vse to vnaša dvomv arhivski proces in ovira možnost preverjanja avtentičnosti, celovitosti in nezatajljivosti zapisa po določenem času. S stališča arhivov obstajajo tri možne rešitve: (1) ohraniti digitalne podpise, (2) izločiti podpise ali (3) zapisati sled podpisa kot metapodatek. Za dolgoročno varovanje avtentičnih digitalno podpisanih

* *Doc. dr. Hrvoje Stančić, Oddelek za informacijske in komunikacijske znanosti, Filozofska fakulteta, Ivana Lučića 3, Zagreb, Hrvaška, kontakt: hstancic@ffzg.hr.*

zapisov je tretja rešitev najbolj realistična. Rezultati projekta InterPARES priporočajo organiziranje digitalnega arhiva na način, da se veljavnost digitalnih podpisov preveri v fazi zajema, informacije o veljavnosti se dodajo metapodatkom zapisov, le-ti pa se ohranijo; kasneje se veljavnosti digitalnih podpisov ne preverja več. Tako se vprašanje verodostojnosti prenese z (digitalno podpisanih) zapisov na arhiv, ki hrani digitalne zapise in njihove metapodatke glede veljavnosti.

Ker pa se še vedno dogaja, da se zapisi hranijo v živih sistemih ali dlje časa pred predajo arhivu, se lahko zgodi, da digitalni podpisi in potrdila ob predaji arhivu že potečejo. Tako smo pred izzivom preučevanja možnosti podaljševanja veljavnosti digitalnih podpisov.

Pomembno je, da arhivisti razumejo mehanizme na področju digitalnih podpisov, da bodo lahko preverili avtentičnost, celovitost in nezatajljivost sporočila, dokumenta ali zapisa in da bodo lahko prišli do odločitve v kontekstu (dolgoročnega) digitalnega varovanja.