InterPARES Trust Case Study

Title and code:		Model for Preservation of Trustworthiness of the Digitally Signed, Timestamped and/or Sealed Digital Records (TRUSTER Preservation Model) (EU31) – **Case Study 1 – digitally signed retirement fund records**
Document type:		Case Study
Status:		Final version
Version:		1.2
Research domain:		Control
Date submitted:		3 Feb 2018
Last reviewed:		3 Feb 2018
Author:		InterPARES Trust Project
Writer(s):		Hrvoje Stančić
Research team:		Elis Missoni (FINA) Hrvoje Stančić (University of Zagreb, FHSS) Andro Babić, Nikola Bonić, Vladimir Bralić, Magdalena Kuleš, Anabela Lendić, Ivan Slade Šilović, Ira Volarević (University of Zagreb, GRAs at FHSS)

Document Control

Version history			
Version	**Date**	**By**	**Version notes**
0.1	4 Jan 2017	Hrvoje Stančić	Initial internal draft
0.2	29 Mar 2017	Hrvoje Stančić	Draft for consultation at EU31 level
1.0	10 Dec 2017	Hrvoje Stančić	Final draft for consultation at EU31 level
1.1	12 Jan 2018	Mats Stengård	Minor improvements
1.2	3 Feb 2018	Hrvoje Stančić	Final version

Table of Contents

Abstract 4
Overview 5
Case study goals 5
Statement of Methodology 6
Description of Context 7
Provenancial 7
Legal 7
Procedural 7
Documentary 7
Technological 7
Interview 8
Phase 1 8
Phase 2 11
Overall Findings 14
Conclusions & Recommendations 15

Abstract

This case study has been conducted in cooperation with FINA – Financial Agency in Croatia between June and October 2016.

The main goals of this case study are (1) to analyse the current use of and state of preservation of digitally signed retirement fund records (e-Regos) held by FINA, (2) to understand the perceived value of the need for archiving of the digital signatures as well as the archiving of the validity of the digital signatures, and (3) to understand how could the expiration of certificates in digital signatures influence the admissibility of records as evidence in the court.

The analysis is focused on the digitally signed records and the preservation of the validity of used certificates in the e-Regos system. Thus the report summarises the procedures with those records related to the case study goals. It could also function as a foundation for further cooperation or additional, more detailed studies.

The study highlights the need for development of a digital preservation strategy and a policy for preservation of the validity of digital signatures. The analysed solution lean on the technical capabilities of the defunct IT system and the information migrated from the records to a database.

Overview

This case study has been conducted in cooperation with FINA – Financial Agency in Croatia, also a national-level Certification Authority (CA), between June and October 2016.

The report uses part of the InterPARES case study report template but the scope of the study is smaller and therefore several headings are excluded.

The objectives of this case study are (1) to better understand the FINA's use of digital signatures, (2) to learn about the FINA's procedures for archiving digital signatures (if existing), and (3) to examine if the research questions set by InterPARES Trust's TRUSTER Preservation Model study (EU31) research team apply.

No detailed analysis of technology of all types of digital records within the FINA has been done but the report summarises the current state of the prioritised and most important areas related to the case study goals. It could also function as a foundation for further cooperation or additional, more detailed studies.

Case study goals

- To analyse the current use of and state of preservation of digitally signed retirement fund records (e-Regos).
- To understand the perceived value of the need for archiving of the digitally signed records as well as the archiving of the validity of the digital signatures.
- To understand how could the expiration of certificates in digital signatures influence the admissibility of records as evidence in the court.

Statement of Methodology

The study was conducted through the interview in two phases. First, the questionnaire was developed. It consisted of 9 sections with the corresponding questions. It was used to cover the first round of the interview. The answers were analysed and discussed among the team members. The additional set of 5 questions was added to the questionnaire in order to fill in the identified gaps. They were used to cover the second round of the interview. This case study report presents the results of both rounds of interviews.

Interviewee (for FINA): Mr. Elis Missoni

Description of Context

Provenancial

Financial Agency (FINA) is the leading Croatian company in the field of financial mediation and the application of information technologies which meet the user requirements. FINA'S greatest advantages are coverage on a national scale, information system well-proved by the most challenging projects of national importance and high professional level of expert teams. Therefore, FINA is able to prepare and carry out different projects – from simple financial transactions to the most sophisticated projects in the electronic business.

With its extensive branch network, FINA covers the entire territory of Croatia following the logic and the intensity of economic activities, while the information systems used to connect the branches enable FINA to meet even the most demanding client demands in a very short period of time. Each branch offers individualized financial and administrative services.

Legal

FINA is one of the leading Certification Authorities in Croatia. They are storing the retirement fund records from a system "e-Regos" (now superseded by a new system) as an outsourced provider. The records are stating how much money was paid into the retirement fund. They have long-term legal value.

Procedural

The study discusses different workflows and procedures related to the handling of electronic records.

A special focus has been put on the digitally signed records and their validity.

To narrow the scope of the study we put focus on the important and large volume of records using digital signatures – the retirement fund records.

Documentary

This case study covers only the retirement fund records.

Technological

FINA is the outsourced third party for storing the records from the "e-Regos" system. The records are available only internally. The system is defunct. The data is transferred to a new database which is available to the users.

Interview

Phase 1

This questionnaire is divided in 9 sections with the corresponding questions. It was used to cover the first round of questions on the status of digitally signed records with the expired certificates held by FINA and intended for long-term preservation.

The records in case are the retirement fund records (e-Regos).

Interviewee (for FINA): Mr. Elis Missoni

Date of the interview: 6 June 2016

Note: Part of the answers are concealed because they were treated as classified by the FINA.

1. Number of records with expired certificates

Q: What is the number of records with expired certificates being stored? Insight needed in order to see how much data we are dealing with.

A: *We are dealing with about a million records.*

2. Number of requests for records with expired certificates

Q: How many requests were made for these records? This can help us decide which records might be more important.

A: *Does not apply in this case because all the data from the records is already in a database and users access the data in the database (using an application).*

Q: Are we dealing with records that are accessible to users?

A: *There have been no cases where the original electronically signed records were needed, only the data from the database was used.*

3. Records importance

Q: Similarly to the previous question, are some of the records more important, should any of the records have a higher priority for preservation/migration etc.?

A: *The records are important for the employers, employees and legislators likewise because they prove how much money was paid into the retirement fund.*

4. Records age

Q: How much time has passed since records certificates expired, and what effect does that have on their potential recertification?

A: *e-Regos has stopped working as a system a year and a half ago (i.e. the end of 2014). A new system has been set up, which means that almost all of the previously signed records are problematic. The records were originally signed with a valid qualified signature and timestamped a few seconds after being signed, however programs today cannot validate these signatures because additional information (CRL lists and certificate chains) is missing. Luckily, the records are part of an IT system, and were validated at the moment of their*

acquisition. FINA claims that at the moment of acquisition the signatures were valid, and this information exists within the system, but not within the digital signatures themselves.

5. Timespan

Q: How much time has passed since certificates for certain records expired? We consider this relevant because a longer timespan means more time for unauthorized access.

A: *Because the records have been stored in a secure way, there is no real threat of an unauthorized access.*

6. Storage and formats

Q: Could you provide insight into the way the records were stored as well as on the formats in which they were stored? What technology was used and how outdated is the technology today? This is important in order to figure out a potential solution for the expired certificates.

A: *The PKCS#7 standard was used during signature creation. This standard has been replaced by the CMS standard into CAdES. The format is the same, but the file attributes differ. The format used is p7s, attached. The p7s is a file which, after being signed, contains the record and the signature. p7s files can only be opened through dedicated programs which are not readily available on standard operating systems. EU's DSS program can validate such digital signatures. However the signature will be validated as INDETERMINATE because information on whether the certificate was valid at the time of signing is unavailable. The system cannot be used for further digital signature augmentation because digital signature augmentation has to be done within the expiration period of the certificates (2 years). One possible solution is adding the "Evidence Record" to the records.*

7. Acquisition

Q: In what way were the records acquired and what was the ingest process? Insight into this will give us more information on how the records were kept and the possibilities for renewing their certificates.

A: *This requires a somewhat lengthy answer, for now I would only say that the records were acquired via safe channels, which cannot be interfered with in any way. The signatures have been validated with a server certificate, which proved their validity. Records which have not been validated are not in the system.*

The information on the internal workflows and procedures related to the handling of digitally signed records were provided in details but requested to be treated as classified. Therefore, only the structure of the provided information is given here, but not the information itself:

7.1. Electronic signing of the file
7.2. File transfer
7.3. Electronic signature verification
7.4. Authorization check
7.5. Time stamping
7.6. Processing
7.7. Electronic signing of the notification/protocol
7.8. Archiving

8. Records management

Q: Who has access to the records? Who manages the records? How does this affect the trustworthiness of these records? How does this affect potential recertification?

A: *Only the authorised FINA personnel have access to the system and they are identified and authorized. The validity of the records is protected by the digital signatures themselves, and if the document has been changed it cannot be validated as the original. The system would inform us that the document has been changed after being signed. Data can be added to the signature itself, and this is an accepted practice because it does not infringe the integrity of the record or signature.*

9. Legal status

Q: What criteria do the expired signatures have to meet in order to be considered as legally valid? Who decides on this?

A: *These records, along with the process information (description of the process and system safety) alongside a signed statement from FINA, could be considered valid in the court. However, there has been no precedence on this topic yet.*

Phase 2

The second and much smaller questionnaire, developed after the analysis of the answers from the Phase 1, consists of 5 questions. It was used to cover the second round of questions on the status of digitally signed records with the expired certificates held by FINA and intended for long-term preservation.

The records in case are the retirement fund records (e-Regos).

Interviewee (for FINA): Mr. Elis Missoni

Date of the interview: 12 October 2016

1. Business usage

Q: Are the problematic records actually used for business purposes? If not, why are they kept, which parties are interested?

A: *All the data contained in the records (electronically signed documents) was extracted and is in a database. For business purposes, that is, for proof of fulfilling the mandatory insurance purposes (second pillar of pension insurance) as required by the law, the data is used from this database. Aligned with the retention and disposition schedule found in the FINA's Archival policy, the records are to be permanently stored. This is because a national law requires it to be stored permanently. Permanent storage is not defined in years.*

2. Legal value

Q: Are these records relevant to current or foreseeable high-value disputes and court proceedings?

A: *Original, electronically signed records have not been needed for court proceedings yet.*

3. Long term preservation

Q: Did you investigate the following as a solution for current or future long-term preservation problems? If yes, are they feasible?

- Re-validation of historical signatures using special software/hardware and/or third party services
  A: *This case study is the first such investigation. No conclusions have been reached yet.*
- Re-signing the records before the expiration of the signatures
  A: *Re-signing is not feasible, since all the signatures have already expired because the certificates used for signing had validity of 2 years. This type of records is no longer used. All records are two or more years old.*
- Using e-notary services
  A: *Our notaries do not offer such a service. They do not have any tools or services regarding e-signature validation or augmentation.*

- Using trusted third party time-stamping and digital archiving services
  A: *Time stamps are not a solution by themselves. Archival timestamps are only good for preventing the existing signature algorithm to be broken. No digital archiving was considered, and our own digital archiving services do not offer a solution for this problem.*
- Blockchain
  A: *We are not aware that blockchain could solve the problem of expired certificate in signature with no proof of existence at the time of signing.*
- Disposal of problematic records (changing legal requirements if necessary)
  A: *It is not up to FINA to dispose these records, as they are not ours. We are contracted as an outsourcing service provider for this system.*
- Validating records at the point of capture into trusted archival system, and afterwards trusting the system to ensure their integrity, usability and authenticity in time
  A: *Yes, we have done exactly that, we trust our system, but in our case, when one of this original, electronically signed document is examined, validation fails.*
- Creating management system for records ensuring solid circumstantial evidence of their integrity and authenticity
  A: *We do not have RMS and we do not plan to have one in the near future.*
- Other (please specify)
  A: *We think that augmentation of expired signatures might be done according to* ETSI EN 319 102-1 V1.1.1 (2016-05) Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures. Part 1: Creation and Validation. *According to* RFC 4998 Evidence Record Syntax norms (Appendix A. Evidence Record Using CMS): *"An Evidence Record can be added to signed data or enveloped data in order to transfer them in a conclusive way. For CMS*[1]*, a sensible place to store such an Evidence Record is an unsigned attribute (signed message) or an unprotected attribute (enveloped message). One advantage of storing the Evidence Record within the CMS structure is that all data can be transferred in one conclusive file and are directly connected. The documents, the signatures, and their Evidence Records can be bundled and managed together." By injecting them with Evidence Record (unit of data, which can be used to prove the existence of an archived data object or an archived data object group at a certain time) would solve our problem.*

4. Cost of preservation vs. risks

Q: Did you evaluate the cost of preservation (in various scenarios) vs. risks (such as fines for non-compliance, damages paid as a result of court cases etc.)?

A: *No, to FINA, managing these records is a payed for service and no risks occurred.*

[1] Cryptographic Messages Syntax.

5. Problem reoccurrence

Q: How sure are you that the problem, once solved, won't repeat in time? (Unsure / Somewhat unsure / Somewhat sure / Sure / Don't know)

A: *We are sure that if we inject the Proof of Existence (POE) in the electronic signatures, they will then always be successfully validated. Another issue is, of course, advancement of technology and weakening of signature algorithms and keys, but that problem is facing all e-signatures and can be solved with Archival Timestamps of greater strength (new algorithms, longer keys).*

Overall Findings

The case study investigated the processes with digitally signed records in a defunct e-Regos system which was transferred to FINA as an outsourcing service. The research showed that the records in the e-Regos system used FINA's (a CA in Croatia) qualified signatures and timestamps. Before the e-Regos system was discontinued, the records were transferred to the FINA who now stores the original digital records locally, i.e. they are not accessible online. However, the information from the records was transferred to an online database and it is accessible there. The digital signatures on the original records cannot be validated any longer because the CRLs and certificate chains from that time are not preserved.

Technological context

FINA claims that:

1) the original records are not modified
2) the signatures were valid at the time of acquisition
3) the confirmation of the validity from the time of acquisition is present in the system, and
4) the records are kept offline under physically safe conditions.

However, it should be pointed out that since the format containing the record and the signature is *p7s, attached* one would need dedicated software, not available for the standard operating systems today, for opening the original records.

Legal context

Taking all that into account, FINA says, if anyone would challenge the authenticity of the information in the online database, they will be able to check that information against the offline original records and establish the truth. The records, the process information and the signed statement should suffice in a legal dispute, but such a case has never happened.

Conclusions & Recommendations

Conclusions

As regards the digitally signed records from the defunct e-Regos system (pension fund records), FINA is an outsourced provider for their permanent storage. Therefore, it will be organised following the FINA's Archival policy.

This case study identified the need for: 1) a common strategy with regards to the use of digital signatures, and 2) a common policy for archival procedures related to them. The existing solutions arise from the technical capabilities of the legacy IT system and the information migrated from the records to a database.

From an archival perspective FINA sees value in the long-term storage of the current state of digital records from e-Regos, acknowledging that the validity of the digital signatures has expired.

The general conclusion from the study is therefore that in this particular case it is too late to try to preserve the validity of the digital signatures since they have already expired.

Digital Signatures: The type of digital signatures used is p7s attached. The p7s is a file which, after being signed, contains the record and the signature.

Value of preservation: This was not fully recognised or clearly stated in any workflow but the study triggered discussions about the need for a focused analysis and a common strategy.

Legal requirements: The law in Croatia requires the pension fund records to be permanently preserved. Therefore, preservation of digital signatures' validity is of interest though not explicitly noted as a requirement by the law.

Archived signatures: The information of the validity of the archived digital signatures is present in the system (since they were acquired while still valid) and stored within the system (not as part of the records).

Preservation of validity: FINA, as the CA whose PKI infrastructure was originally used for signing the records, claims that, if necessary, can establish the truth by using the support process. This support process was not tested or evaluated during this case study. No other expressed strategy or a proprietary process being able to recover or prove signature validity was noted as existing.

Recommendations

When a digital archive decides to ingest digitally signed records it should have a strategy for their (long-term) preservation and a policy how the validity of digital signatures are to be preserved. As it was shown earlier, the value of the signature's validity should not be seen as less important than the value of other attributes or information in a record. It would be strongly advisable to preserve the validity if it can be preserved without unreasonable costs.

When deciding to ingest the digitally signed records in the digital archive a choice should be made how the records will be preserved:

- with digital signatures – deployment of considerable means to preserve the necessary mechanisms for validating the signatures,
- without the digital signatures,
- with the information about the validity of the digital signatures at the time of ingest added to the metadata, or
- with the digital signatures whose validity information is registered in the blockchain (TRUSTER's VIP (Validity Information Preservation) solution: TrustChain).

In any case, it would be highly recommendable to specify and implement a working procedure for the transfer to the archive / ingest process which supports the secure transfer and keeps the validity of the signature intact until the record is in the archive.