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 2 – digitally signed e-tax records**
Document type:		Case Study
Status:		Final version
Version:		1.2
Research domain:		Control
Author:		InterPARES Trust Project
Date submitted:		3 Feb 2018
Last reviewed:		3 Feb 2018
Writer(s):		Hrvoje Stančić
Research team:		Željko Mikić (TechEd Consulting Ltd.) 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	22 Apr 2017	Hrvoje Stančić	Initial internal draft
1.0	22 Dec 2017	Hrvoje Stančić	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

This case study has been conducted in cooperation with TechEd Consulting Ltd. and Croatian Tax Administration, between January and April 2017.

The main goals of this case study are (1) to analyse the current use of and state of preservation of digitally signed records held by the Croatian Tax Administration, (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 focussed on the digitally signed records and the preservation of the validity of used certificates in the e-TAX records. 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 current solutions lack records management component, digital preservation policy, digital archive and the system in place cannot satisfy current legal requirements for long-term preservation.

Overview

This case study has been conducted in cooperation with the Croatian Tax Administration, between January and April 2017.

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 Tax Administration's processes with the digitally signed records, (2) to learn about the Tax Administration'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 Tax Administration 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 submissions of annual income tax (e-TAX).
- 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 research was conducted by using the questionnaire. The questionnaire that was used was the same questionnaire developed through two phases of the Case Study 1. It consisted of 11 sections with the corresponding questions. The questionnaire was sent to the Tax Administration (TA) and the questions, where necessary, were discussed with the TA representatives. The answers were later analysed and discussed among the team members. This case study report presents the results of the research.

Description of Context

Provenancial

"The Tax Administration is the administrative organization within the Ministry of Finance whose basic task is to implement tax regulations and regulations concerning the payment of obligatory contributions."[1]

Legal

"All residents are obliged to participate in the settlement of public expenses in accordance with their economic abilities. The tax system is based on the principles of equality and equity."[2] The records covered by this case study are the submissions of annual income tax and the JOPPD (Report on receipts, income tax, surtax and contributions for compulsory insurance) forms which 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 the validity of digital signatures.

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

Documentary

This case study covers the digitally signed records.

Technological

The Tax Administration records rely on the third party digital signatures. Part of the records are available only internally (2006-2013), and the rest is available publically online (2014 onwards). The data is stored in database and file system.

[1] The Republic of Croatia, Tax Administration, https://www.porezna-uprava.hr/en/Pages/default.aspx
[2] Ibid.

Research

This questionnaire is divided in 11 sections with the corresponding questions. It was used to investigate the status of and the procedures with digitally signed records with the expired certificates held by the Croatian Tax Administration and intended for long-term preservation.

The records in case are the submissions of annual income tax.

Research perioud: January – April 2017.

1. Number of documents with expired certificates

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

A: – *(The exact number of documents with expired certificates was not revealed.)*

2. Number of requests for these documents with expired certificates

Q: How many requests were made for these documents? This can help us decide which documents are more important.

A: *There is no official statistics on the requests for these documents. The system enables creation and delivery of documents but does not log the number of requests per document.*

Q: Are you dealing with documents that are accessible to users?

A: *Yes.*

3. Document importance

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

A: *There is no concrete information on the importance of the documents available. The law requires, for example that the Form JOPPD (Report on receipts, income tax, surtax and contributions for compulsory insurance) should be preserved for 100 years.*

4. Document age

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

A: *Certificates are valid for two years. After that they expire. The earliest documents in the system are dating from 2006 and there might be expired certificates in the system from that time. FINA should have the historic CRL lists so that recertification might be possible at the time of archiving if the original signature might be 100% checked. CRL lists might be obtained by request.*

5. Document timespan (how much time has passed since the certificates have expired)

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

A: *Since the system is dating back from 2006, it is at least 10 years.*

6. In what way were the documents stored, what formats were used?

Q: Could you provide the insight into the way the documents 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 tax forms are stored either in the data bases or in the file system. The format is XML. The XMLDSig type of signature was used until 2013 when it was upgraded to XAdES type of digital signature. SHA-1 hash algorithm is used along with RSA cryptographic algorithm for digital signature. SHA-1 is considered obsolete today and it is recommendable to change to the SHA-2 algorithm.*

7. Document acquisition process

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

A: *The documents (forms) were submitted by the taxpayers using internet. They are kept in the data bases or file system.*

8. Document management of the files with expired digital signatures

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

A: *The taxpayers, the taxpayers' assignees, and the Tax Administration employees have access to the documents. APIS IT*[3] *is responsible for the management of the documents at the system level. The documents are stored in a secure way and no changes are possible. The trustworthiness is guaranteed by the physical access control to the production system. The recertification should be possible because the users could only submit the documents and cannot change them once they are submitted (the system only ingests documents without the possibility of change or deletion).*

9. Legal status of the expired signatures

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

A: *The legal validity is (in Croatia) regulated by the Electronic Signature Act (n.b. from 1 July 2017 it is derogated by the European e-IDAS regulation) and the Electronic Document Act.*

10. Business use

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

A: *Electronic documents are used for fulfilling the tax obligations coming out from several regulations. Some forms, like the Form JOPPD, are important because they are used to*

[3] Outsourced provider – the Information Systems and Information Technologies Support Agency, Croatia.

calculate the pensions. Therefore, it is important to keep them long enough – until the currently employed citizens are retired.

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

A: *The current records are used in the legal disputes – they are printed on paper (i.e. the copies are being made) and the paper printout is then authenticated by the Tax Administration.*

11. 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?

a. Re-validating of historical signatures using special software/hardware and/or third party services
   A: *It might be feasible only if FINA*[4] *would make available the historic CRLs – than the records could be re-signed using newer and stronger algorithms. The appropriate CRL would be included, in order to make the digital signature of the original document verifiable, along with the CRL used at the time of re-signing. It would be recommendable to use archival XAdES type of digital signature.*
b. Re-signing the records before the expiration of the signatures
   A: *This would solve the problem of expiration of the certificates. Before the certificate expires the system should certify the document with a new signature which includes all the necessary data for later verification.*
c. Using e-notary services
   A: *No.*
d. Using trusted third party time-stamping and digital archiving services
   A: *No.*
e. Blockchain
   A: *No.*
f. Disposal of problematic records (changing legal requirements if necessary)
   A: *No.*
g. 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: *No.*
h. Creating management system for records ensuring solid circumstantial evidence of their integrity and authenticity.
   A: *This is a general question about archiving of electronic documents. We were considering building an archival system which would automate what was mentioned under a).*

[4] FINA – Financial Agency, Certificate Authority (CA) in Croatia.

i. Other (please specify)
A: *It might be a good option to use the form of digital signature containing all needed information for long-term preservation. However, that might become an issue because of the increased storage requirements – each document would need additional data like CRL, certificate of the issuer etc., but that would solve the long-term preservation issue.*

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.*

Q: How sure are you that the problem, once solved, won't repeat in time?

A: *We are somewhat sure. However, it is hard to say because the technology is constantly advancing and we do not know which new problems might show up.*

Overall Findings

The case study investigated the processes with digitally signed records in custody of the Croatian Tax Administration. The research showed that the records have XML signatures, qualified signatures and timestamps. The digital signatures on the original records dating from 2006 cannot be validated any longer because they have expired. In order to check them the Tax Administration should request the CA which originally issued keys for digital signatures to provide the old CRLs and certificate chains from that period. However, they are not preserved. Neither the information on the validity of digital signatures nor other information from or about digital signatures were recorded as metadata[5].

Technological context

The Tax Administration claims that:

1) the original records are kept in the data bases or file system
2) the documents are stored in a secure way (by an outsourced company) and no changes are possible
3) users can only submit the documents and cannot change them once they are submitted
4) the trustworthiness is guaranteed by the physical access control to the production system.

However, it should be pointed out that:

1) the records management system is not implemented
2) there is no digital preservation policy in place
3) there is no digital archive
4) the information from the digital signatures is not kept as metadata
5) records use now obsolete SHA-1 with RSA cryptographic algorithms for digital signatures
6) in the case of legal dispute digital records are printed and physically authenticated.

Legal context

Some digitally submitted forms, like the Form JOPPD (Report on receipts, income tax, surtax and contributions for compulsory insurance), should be preserved for 100 years.

Currently, when the digital records held by the Tax Administration are needed as evidence in legal disputes they are printed and the paper printout is authenticated.

[5] The authenticity of the whole set of records can be established by a court in the basis of available circumstantial evidence. This is usual practice in common law countries which, unfortunately, is not widely adopted in continental law countries.

Conclusions & Recommendations

Conclusions

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 current solutions keep documents stored in the database and in the file system. Neither is the records management system in place nor is the digital preservation policy developed. The solution for digital archive is non-existent. However, the survey showed that there is an understanding that all three should be developed and implemented.

From an archival perspective the Tax Administration understands the legal requirements and the value of the long-term preservation of digital records, acknowledging that the validity of the digital signatures of part of the records 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 older than two years since they have already expired.

Digital Signatures: The type of digital signatures used are XMLDSig (2006-2013) and XAdES (2013 onwards). The digitally signed records use SHA-1 with RSA cryptographic algorithms.

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 some of the records to be preserved for 100 years (e.g. the Form JOPPD). 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 not present in the system. However, the signatures had been valid at the time of signing because otherwise the submissions of annual income tax would not have been accepted.

Preservation of validity: The Tax Authority claims that the historical signatures might be re-validated only if the CA which issued keys for original digital signatures provides sufficient information (e.g. historic CRLs). This 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

The records management system, the long-term digital preservation policy and the digital archive should be developed and implemented. The records with still valid digital signatures should be ingested in the digital archive and the information on the validity of the signing certificates should be kept and preserved. Signature's validity should be seen as important as other attributes or information in a record. A cost-benefit analysis of the preservation of the validity should be done to see if the validity can be preserved without unreasonable cost.

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.