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 3 – digitally signed medical records, procurement and supplier contracts, official political decisions and minutes of meetings**
Document type:		Case Study
Status:		Final
Version:		1.3
Research domain:		Control
Date submitted:		3 February 2018
Last reviewed:		27 January 2017
Author:		InterPARES Trust Project
Writers:		Mats Stengård, Enigio Time AB Hans Almgren, Enigio Time AB Hrvoje Stančić, University of Zagreb
Region Skåne participants:		Sofie Idberg, Region Skåne Daniel Hedman, Region Skåne Åsa K Nordström, Region Skåne Kerstin Belin, Region Skåne Christian Jarnekrans, Region Skåne
Research team:		Mats Stengård, Enigio Time AB Hans Almgren, Enigio Time AB Hrvoje Stančić, University of Zagreb

Document Control

Version history			
Version	Date	By	Version notes
0.9	11 Dec 2016	Mats Stengård, Hans Almgren	- First final internal draft
1.0	19 Dec 2016	Hrvoje Stančić	- Case Study improvements
1.1	15 Jan 2017	Mats Stengård	- Review and update from comments - Update from Region Skåne answers in mail 19 Dec 2016
1.2	27 Jan 2017	Hrvoje Stančić	- Final review
1.3	12 Mar 2017	Mats Stengård	- Updates and corrections from comments by Region Skåne

Table of Contents

Abstract 4
A. Overview 5
Case study goals 5
B. Statement of Methodology 6
C. Description of Context 7
Provenancial 7
Legal 7
Procedural 7
Documentary 7
Technological 8
D. Overall Findings 9
Medical Records 9
Tenders, Procurement & Supplier contracts 10
Political decisions & meeting minutes 11
E. Conclusions & Recommendations 12
Conclusions 12
Recommendations 12

Abstract

This case study has been conducted in cooperation with Region Skåne between June 2016 and November 2016.

The main goal of this case study is to examine the Region's use of digital signatures, the way to archive digital signatures and if the research questions of InterPARES Trust EU31 (TRUSTER) apply.

The report summarises the current state of the prioritised and most important areas related to the case study goals. It can also function as a base for further cooperation or studies.

The study highlights the need for a common strategy for Region Skåne with regards to the use of digital signatures and a common policy for archival procedures related to those. The current solutions appear to be more derived from the technical capabilities of the used IT systems and not from specifications based on the business and legal requirements.

When proper digital signatures are created for the records, a proper strategy for preserving the validity of digital signatures should also be made if technically possible. If the validity can be preserved without unreasonable cost it would be strongly advised.

A. Overview

This case study has been conducted in cooperation with Region Skåne – the county council of the Skåne County of Sweden and the Region Archive between June 2016 and November 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 main goal of this case study is to examine the Region's use of digital signatures, the way to archive digital signatures and if the research questions of InterPARES Trust EU31 (TRUSTER) apply.

No detailed analysis of technology of all types of digital records within the Region 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 base for further cooperation or studies.

Case study goals

- To analyse the current use of signatures (physical and digital) in different workflows and type of records at Region Skåne.
- To understand the perceived value of the need for archiving of the digital signatures and digitally signed records as well as the archiving of the validity of the digital signatures.
- To know if and how the digital signatures are currently archived.

B. Statement of Methodology

The study was conducted through analysis of the provided material from the Region as well as through questions and discussions in several Skype meetings and mail conversations with Region Skåne participants. An important component for information gathering was a half-day workshop held at Region Skåne facilities in Malmö, Sweden.

Input for most subsequent meetings and discussions were produced in the workshop where material was gathered and structured from the following agenda.

1. Identification of
    a. records/content types/workflows
        i. where timestamps/seals/signatures exists/ought to exist (both physical & digital)
    b. general legal dependencies
2. Analysis & discussion
    a. created physical/digital
    b. appraisal, time horizon
    c. any current records where validity needs to be extended?
3. Challenges & risks
4. Prioritisation
    a. focus on most important areas for more analysis
5. Summary & planning

Participants from Region Skåne:

- 2 archivists,
- 1 lawyer,
- 1 information manager,
- 1 information strategist.

C. Description of Context

Provenancial

Region Skåne is the county council of the Skåne County of Sweden.

The population of ca. 1 250 000 is about 13% of Sweden's total.

The Skåne County was formed in 1997 by the merger of former Kristianstad County and Malmöhus County established in 1719. Region Skåne was formed in 1999 by the merging of the two administrative county councils of the province of Skåne; Kristianstad County and Malmöhus County, which were established in 1863.

Healthcare is Region Skåne's dominant area of activity.

Region Skåne is responsible for healthcare and public transport, business development, culture, infrastructure, social planning and environmental and climate-related issues in Skåne.

Legal

The seat of residence for the Skåne Governor is the town of Malmö. The headquarters of Skåne Regional Council is the town of Kristianstad.

With 34,000 employees, Region Skåne is one of Sweden's biggest employers.

It is a self-governing administrative region, funded by taxes, which is governed by a Regional Council of 149 members who are directly elected by the inhabitants of Skåne.

The Regional Council makes decisions regarding budget and direction for Region Skåne's various operations. Most decisions are based on suggestions made by the Regional Executive Committee, which is appointed by the Council.

Procedural

The study discusses different workflows and procedures related to the handling of electronic records both active and archived within the Region Archive.

A special focus has been on the use of digital signatures for different types of records and the need for archiving of the digitally signed records and the validity of digital signatures.

To narrow the scope of the study we put focus on the most important and the largest volume of records using signatures (priority by Region Skåne) – medical records, supplier contracts and political decisions and meetings.

Documentary

Region Skåne keep documents as per the Archives Act, in order to respect the public's right to access public documents. They also look after the needs of research, own operations, and the legal system.

The Region Archive is part of the Archive Centre South (Arkivcentrum Syd) in Lund – Scandinavia's biggest archival institution.

Region Skåne Archive operates in a mixed digital and analogue environment but has the ambition to move as much records as possible to digital storage.

Health care information, such as medical records, constitutes almost 80% of the archive's materials. But there are also minutes and other documents concerning political processes, history of the county council, blueprints, education transcripts, maps etc.

Technological

Complex IT portfolio, around 1 000 systems, 100-150 will be replaced by a new system, which is currently being specified.

Region Skåne archive and external consultants develop solutions for delivery between business and document managements systems and e-archive. Records are delivered to the e-archive via own Region Skåne specific delivery specifications (submission information package) to the e-Archive.

The archive currently is an in-house built e-archive solution based on OEF (Open E-archive Framework).

e-Service card (RSID card)

The RSID-card is an important technical component used for security and identification at Region Skåne. It is an electronic identity card (eID card) including Region Skåne's service certificates (also called a SITHS card).

The card is to be used by all employees for all identification within Region Skåne.

The cards and service certificates increase security significantly during login to IT systems. RS cards and its certificates are normally valid for 5 years for permanent employees. Temporary employees receive cards of a shorter duration.

D. Overall Findings

Authorisations and signatures are used in many of the workflows and created records. Multiple types of signatures are used; physical signatures (scanned), system authorisations and also qualified digital signatures.

Signatures are used for, among others:

- Medical records, dental care, doctor's certificates
- Procurement and contracts with suppliers, construction projects
- Powers of attorney,
- Digitally signed e-mails,
- Accounting/bookkeeping, employee agreements
- NDAs
- etc.

Together with Region Skåne it was decided that this case study should focus on the most important and the largest volume of records using signatures:

1. Medical records
2. Procurement and supplier contract
3. Official political decisions and minutes of meetings

Medical Records

Medical records are the biggest record type created and handled by Region Skåne. It constitutes about 80% of the records stored in the Region Archive.

Legal context

Record keeping and information management within health care in Sweden is regulated by the "Patient Data Law" (PDL). The points listed below are some important statements in this law related to the case study questions.

- Preservation at least 10 years, government can decide that certain type of records should be preserved longer than 10 years.
- Strong authentication should be used for accessing medical records.
- The caregiver must ensure that there are procedures for the signing of notes and confirmation of actions relating to patient care and treatment.
- Caregivers who are connected to a system for coherent records must decide on common procedures for signing and securing data.

Required legal preservation, as seen, is at least 10 years but recommendations in Sweden for medical records are to assume a strategy of "permanent retention". Region Skåne applies this and there is no process for disposition with regards to the medical records.

No specific requirement on the "quality" of the digital signature from a technical perspective is described within the law, only the statement of "strong authentication". "Strong authentication" is defined as a requirement that identity should be controlled in at least two different ways before access to records is granted. The "RS-Card" identification together with a password fulfils the requirement for "strong authentication" according to the definition.

Technological context

Mainly two different business systems are used today for creation of medical records – PMO is used for primary care, Melior is used for specialist care.

Both systems have the capacity to use the RSID-Card technology for strong authentication and digital signatures using HCC (Health Care Certificates). But currently it is not used consistently for both or for all operations.

To login to PMO RSID-Card authorisation is required. Currently though the digital signature code from the card is not used for signing a journal because the login authorised by the card is considered as sufficient authorisation. On the other hand for signing, for example, medical e-prescriptions it is used.

Melior, like described, has the capacity to sign with the RS-Card but also have the possibility to login with username and password. Both are used but username and password is most common. When login in with RSID-card the signing code for the card is used for signing within the system, otherwise the password for the user is used. Medical e-prescriptions are always signed with a PIN-code. The plan at the time of study was that the use of RSID-Card would be introduced more generally also for the Melior users during late 2016.

Each sign off (signature) in the systems require at least the application of a PIN code, some sign-offs does only require the logged in state and the presence of the card.

The qualified digital signatures created using the RSID-Card are of PKI type with certificates that expire (in up to 5 years).

Preservation context

The e-Archive currently holds medical records for 1 300 000 persons but so far no digitally signed records have been ingested to the e-Archive.

No medical journals have been archived from the current journal systems PMO or Melior. The chance to define a new common strategy and process for how to handle the records and digital signatures when journals should be archived is therefore possible.

Tenders, Procurement & Supplier contracts

As Region Skåne is a large, tax financed institution tenders, procurement and supplier contracts are an important part of the operation and are archived.

Legal context

The law for public procurement apply, and required legal preservation is depending on the type of contract.

In some cases Region Skåne applies “permanent retention” in same way as for medical journals, but not for all, it depends on type of contract.

Technological context

Both previous and current IT system (CSign and TendSign) use qualified digital signatures for the signing of contracts. The service supplier CSign delivers the digital signatures to both systems, signatures are of PKI type and thus certificates expire. At the time of this study about 1500 digitally signed records where active in TendSign (not archived).

Preservation context

1500 digitally signed records have been transferred from the previous CSign system to the e-Archive. The digital signatures associated with the signed records are archived as checksummed “metadata”.

The preservation of the signatures' validity in this case "might" be said to follow the "system-dependency"[1] policy recommended by the Swedish National Archives. Region Skåne have not had a conscious decision to follow the policy at the time of ingestion of the records but the validity according to this policy could be verified with some more detailed analysis – most importantly by evaluating the technical procedure of record and signature ingestion to the archive from the business system.

Political decisions & meeting minutes

Lots of the operation within Region Skåne requires political meetings and decisions, thus minutes from these meetings and decisions are an important part of the records handled by the Region and the Archive.

Legal context

Required legal preservation of these types of records is flexible. Region Skåne applies "permanent retention" on all political decisions and meeting minutes.

Technological context

Today these signed records are archived on paper. Unsigned digital copies are published for the general public.

Region Skåne is currently in the process of digitising this flow and intend to use digital signatures. A new system is thus being specified and evaluated. Because of this, an analysis of the process and type of digital signature needed might be important.

Preservation context

The new system has not yet been fully implemented and digitally signed records are yet to be archived. The chance to define a new common strategy and process for how to handle the records and digital signatures is therefore possible.

[1] "System dependency" is described in the report "Production and preservation of electronic signatures" produced and published by the Swedish National Archives. In essence it refers to a system in which technical and/or systematic measures are taken so that they together create a system that can validate a data object by ensuring that the data object has not changed and that data object was isolated until preserved.

E. Conclusions & Recommendations

Conclusions

Region Skåne has a policy of permanent retention (no appraisal) for all record types prioritised in this study.

This case study highlights the need for a common strategy with regards to the use of digital signatures and a common policy for archival procedures related to those. The current solutions seem more derived from the technical capabilities of the used IT systems and not from specifications based on the business and legal requirements.

From an archival perspective Region Skåne sees value in the long-term preservation of the validity of the digital signatures if technically possible. The cost for such a solution and the possibility of integrating it within the current infrastructure is of course something that needs to be weighed against that value.

The general conclusion from the study is therefore that for certain applications and record types within the business of Region Skåne there is a value of preserving the validity of digital signatures, if it is technically possible, and the cost is not too high.

Digital Signatures: Signatures of many different kinds are used in many different ways in all types of records and systems – both qualified digital signatures and proprietary. System specific solutions are used as well as scanning of the physical signatures.

Value of preservation: This was not fully recognised or clearly stated in all workflows but the study triggered discussions about the need for a focused analysis and a common strategy. The group conclusion was that if it was technically possible there was no clear reason not to preserve the validity when all other parts of a record should be retained.

Legal requirements: A medical journal should be preserved for at least 10 years, thus well passing the expiration of any certificate. The recommended Swedish policy within health care is "permanent retention" of medical records (no appraisal), which Region Skåne follows. Therefore, preservation of digital signatures' validity is of interest though not explicitly noted as a requirement by the law.

Archived signatures: Records signed by qualified digital signatures and the digital signature itself have been archived in different ways, without an agreed stated common strategy. Region Skåne expressed an interest in better understanding how this should be created, planned and implemented, preferably without a specific supplier dependency. Today as described by Region Skåne, because a lack of policy and because of technical limitations archived digital signatures are kept as metadata together with archived digitally signed record. If system and ingest procedures from business system to archive is secure, the validity of signatures might be considered as preserved according to the "system dependency" policy defined by the Swedish National Archives.

Preservation of validity: When a signature is archived today it is not considered for verification of validity, only saved as metadata. If a signature might be needed for validation in the future they are currently kept in the source system. No other expressed strategy or a proprietary process being able to recover or prove signature validity was noted as existing at the Region currently.

Recommendations

Region Skåne should describe and agree on a common strategy for how and when qualified digital signatures should be used. Both in what use cases a signature should be created and

when and how it should be saved and ingested together with its record to the archive. It should be a stated aspiration that qualified digital signatures are used in a consistent way in all workflows and systems requiring sign-off and signatures.

When a new IT system is procured and integrated a specification should exist on what is required from the business and legal perspectives to adhere to the stated strategy regarding signatures.

All current business systems, used for the most prioritised records, have the capability to use and create qualified digital signatures based on the RS-Cards. Because of this the Region Skåne could build mainly on the existing authentication infrastructure for employees and use Mobile Bank ID for others. The RS-Cards are perfect for creating "strong authentication" and qualified digital signatures.

When proper digital signatures are created for the records, a proper strategy for preserving the validity of digital signatures should also be made if technically possible. 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. If the validity can be preserved without unreasonable cost it would be strongly advised.

The Region Skåne should make a choice of how the digital signatures should be preserved:

- as metadata only (trying to preserve secure system dependency in all steps)
- a possible TRUSTER approach.