Requirements for Evidential Value for the Assessment of the Trustworthiness of Digital Records over Time

Jianqiang Ma*†, Habtamu Abie†, Torbjørn Skramstad* and Mads Nygård*
* Department of Computer and Information Science
Norwegian University of Science and Technology, Trondheim, Norway
Email: {majian, torbjorn, mads}@idi.ntnu.no
† Norwegian Computing Center, Oslo, Norway
Email: {Jianqiang.Ma, Habtamu.Abie}@nr.no

***Abstract*—The issue of trust in the management of digital records has been a topic of research for a number of years. During this time most researchers have concentrated on the nature and meaning of the record itself, rather than the potential use of the record as evidence of the originators' origins, functions, and activities. Through a comparison of trust in the real world and trust in the digital world, we demonstrate the importance of evidential value in the assessment of the trustworthiness of a record. In this paper we investigate, identify and specify the requirements for evidential value, based on our life cycle model of the record. Finally, we show briefly how these requirements can be used in the assessment of the trustworthiness of records in long-term storage.**

I. Introduction

Earlier, people used paper documents to store information, using pens and papers. Now, as the information technology is growing dramatically, people more and more have to rely on electronic documents. People write diaries in digital form, using a digital camera to take photos and upload them to their computers, even publish them to the Internet. When people shop in supermarkets, their purchasing records are logged into the banking system and in data repositories. Enterprises need to store their data in digital repositories. Even for individuals, it is not enough to only store their long term data in personal computers. That is, the disks in those computers may not be large enough, or the personal computers are not intended for long term storage usage. Then comes the question: how can we trust these repositories? When we store some data into a repository and retrieve them later, how can we trust that the data are still the same as before without being tampered? Many researchers and practitioners have contributed to this field, mostly dealing with the repositories, e.g. how to operate the repositories and how to make them trustworthy [1], [2]. Few of them [3], [4] have researched the use of the records as evidence of the originator's origins, functions and activities. Therefore, we focus on the value that a record has, specifically the evidential value, and use this value to assess and calculate the trustworthiness of the record.

In this paper, we concentrate on developing the requirements for evidential value, and briefly explain how to assess the trustworthiness of a record using these requirements. The assessment method and preservation issues are topics of our forthcoming papers.

This work is part of the Trust work package of the LongRec (Records Management over Decades) project [5], which is a three years research project partly funded by the Research Council of Norway. The primary objective of the LongRec project is the Persistent, Reliable and Trustworthy Long-Term Archival of Digital Documents, with Emphasis on Availability and Use of Documents. In this project, the research on long term record preservation has been divided into four work packages; Find, Read, Trust and Understanding. The Find work package concerns records retrieval; the Read work package focuses on records preservation covering records storage; the Understanding work package deals with the records semantic value, and the Trust work package cares about the assessment of records' trustworthiness over time.

The rest of this paper is organized as follows. We first assess other researchers' definitions of evidential value, and come up with our definition in Section II. In Section III, we introduce the scenario of trust in the digital world. By comparing with trust in the real world, this section demonstrates the importance of evidential value and the use of evidential value to measure records' trustworthiness. In Section IV, we illustrate the different phases of a record's life cycle, and how these phases are used to categorize the requirements for evidential value is presented in Section V. We briefly explain how the evidential value can be used to assess the trustworthiness of a record in Section VI, and finally, conclusions and suggested future work are given in Section VII.

II. Evidential Value

One of the issues concerning evidential value is the lack of a standardized definition of the use and of the key concepts involved. Different interpretations of the term abound. Definitions differ with the viewpoint of the definer, and several are given in this section, including our own.

In accordance with Schellenberg's Appraisal Taxonomy [6], [7], preserved records have two types of value, categorized as

978-1-4244-5113-5/09/$25.00

primary and *secondary* value respectively. The primary value of a record is the value that the record has for the creator, who will use the record for legal, fiscal or administrative purposes, and as necessary for the continuation of business. The secondary value of a record is the value the record has for persons or entities other than the creator, including public and private users. David and Roderick [8] mentioned that *"research or historical values are generally designated as the secondary value"*, Gerald [9] stated that the secondary value of a record is *"the main concern of archival appraiser"*. Given that we do research as a user of the record, not as the creator, therefore, we concentrate on a record's secondary value. Schellenberg [10] further classified a record's secondary value into two types, i.e. *evidential value* and *informational value*. He elaborated that informational values are "the values that attach to records because of the information they contain", and evidential values are "the values that attach to records because of the evidence they contain of organization and function". Given that we are concerned with the value which can be used to assess the record's trustworthiness, we pay our attention only to the evidential value in the rest of this section.

There have been numerous attempts to define what evidential value is more specifically, however, they haven't come up with an agreed upon definition which is widely adopted as a standard.

Some of the definitions [11]–[15] were given on an organization's perspective. One of the definitions is:

> *Evidential value refers to the significance of the information a record provides about a government office and the function that produced it. It is the evidence of an agency's existence and achievements. Records that document significant government functions, policies, and decisions have evidential value. [11]*

Some of the definitions [16] underscored evidential value's ability to be used as evidence. The definition is:

> *Evidential value refers to the documents' ability to serve as legal or historical proof of an activity, event, or occupation. (1). High-value materials are the originals in an unmodified form. (2). Moderate-value collections might include some records of legal value, such as birth certificates or legal copies of land records. (3). Low-value materials are modified records or copies. [16]*

And some of the definitions [17]–[20] depicted evidential value with focus on the creation of the record. One of the definitions is:

> *The quality of records that provides information about the origins, functions, and activities of their creator. Evidential value relates the process of creation rather than the content (informational value) of the records. [18]*

However, none of them is good enough to be used to research on assessment of records' trustworthiness. The first and second definition have not put attention on the records, while the third definition limits to the creation of the record, ignores the historical information pertaining to the record. Thus, we proposed our definition [21] which focuses on the records and also includes the historical information. Our definition is:

> *"Evidential value is the quality of the record that provides a legal proof, historical proof, authentic evidence, and adequate evidence about:*
>
> - *the origin of the record,*
> - *the creator of the record,*
> - *the creation of the record from different perspectives,*
> - *the history of events and topics associated with the record, such as activities, functions, policies, operations etc."*

In this definition, we not only consider the creation of the record, but also the record's history, which will later be used to assess the record's trustworthiness. It is therefore essential that the history of the record is documented in a way that can be inspected, validated and reasoned about by authorized users so that it is possible to check and ensure that records have not been modified, abused or tampered with. In our research, we will not investigate on the legal perspective of the evidential value.

III. Trust from Real World to Digital World

In the previous section, we assessed the numerous definitions of evidential value and proposed our own. In this section, we use a scenario to illustrate why it is vital to document the history of events and topics associated with the record as evidential value. We first state the process of building and maintaining trust in the real world (people's trust in people), and then further demonstrate how this process works in the digital world (people's trust in records).

A. Trust in the Real World

We suppose that Alice and Bob are two persons, and Alice is going to assess Bob's trustworthiness to her. When Alice meets Bob for the first time, she doesn't know him. Therefore, she would try to obtain more knowledge about him, by getting suggestions from others, or by observing Bob's behavior. Alice would give Bob an assessment of his trustworthiness to her at first, and then, along with their interaction, she would adjust the trustworthiness based upon further information she obtained. This adjustment could either increase or decrease. After some time, if the trustworthiness goes down to complete no trust (numeric 0), meaning that Alice will not trust anything of Bob's expressions, then she will probably stop her interaction with Bob. While, if the trustworthiness goes up to complete high trust (numeric 1), she will trust anything Bob expresses. However, even if the trustworthiness is very high, it is still possible that it will be changed by Alice in certain situations, such as lack of interaction for years, or advised by others about Bob's highly untrustworthy. This process is shown in Figure 1.

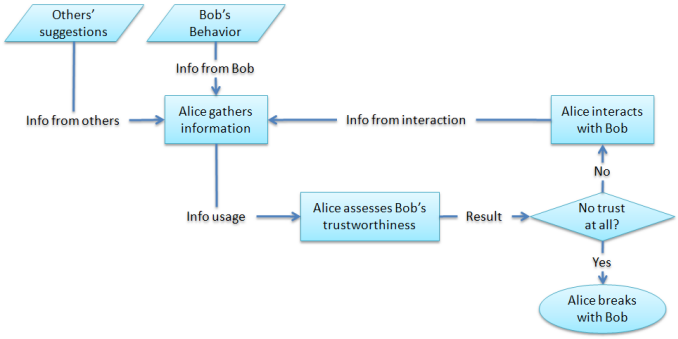

Fig. 1. Trustworthiness assessment process in the real world.

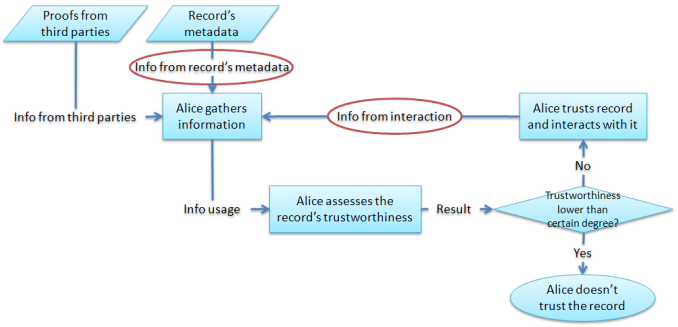

Fig. 2. Trustworthiness assessment process in the digital world.

From this scenario, we conclude some important issues which are good references for us to express trust in the digital world:

- The assessed trustworthiness is not just 0 or 1, it is a linguistic value (e.g. very high trustworthiness, high trustworthiness, medium trustworthiness, low trustworthiness, no trust), which can be mapped into a numeric value between 0 and 1, called the *degree of trust*.
- Alice assesses the degree of trust using the information she got about Bob.
- The information used to assess the trustworthiness could be gathered by Alice's observation and/or by others' suggestions.
- Alice adjusts her assessment of Bob's trustworthiness along with the information increase.

B. Trust in the Digital World

Trust in the digital world is similar to trust in the real world. As in the real world trust, when a person (to facilitate the explanation, we still use Alice) needs to assess a record's trustworthiness, she first needs to find related background information about the record. This background information is called *metadata*, which is "data about other data" [22], we will not deal with the different definitions here. The metadata includes information like *time of creation*, *author*, *modification logs*, and so on. In addition, the proofs (by using digital signatures) from a third party could also be included in the metadata. After collecting the useful information, Alice will assess the trustworthiness of the record. She will work out trust degree of this record, and then make her decision on whether to trust the record or not. Note that, until now, Alice didn't read the content of the record. The assessment was made based on the metadata about the record alone. When she decides to trust the record, she starts to read the content, and then modifies it or checks relevant context. By Alice's actions, which we called interaction with the record, further information will be obtained. Later, she will adjust the record's trustworthiness based upon this information. The adjustment could either increase or decrease. Figure 2 shows the trustworthiness assessment process in the digital world.

Comparing Figure 2 with Figure 1, we see that they are using a similar process to assess the trustworthiness of assessee, the only difference is who the assessee is, a digital record or a person. Based upon the important points we have elaborated in the previous section, we conclude that:

- The assessed trustworthiness of the record is a degree of trust, not just 0 and 1.
- The assessment was carried out using information about the record.
- The information used in the assessment is gathered from the record's documented history and/or others' suggestion (digital signature from third parties etc.).
- The record's trustworthiness is adjusted along with information obtained from further interactions.

As we highlight in Figure 2, in order to conduct the assessment of the record's trustworthiness, it is important to have information of the record from both the metadata and further interactions. Given that Alice's interaction with the record will be documented as historical information, therefore, combining with the last three points listed above, we conclude that it is essential to have the historical information of a record in order to assess its trustworthiness. Recalling the definition of evidential value from Section II, we see that the evidential value provides evidence about the history of events and topics associated with the record. Hence, in our research, we will use evidential value to achieve trust assessment to digital records.

IV. Record's Life Cycle

In the previous two sections, we demonstrated what evidential value is, and why it is important for the assessment of the record's trustworthiness. In order to specify which elements shall be included in the evidential value, we first need to know how a record lives in the digital repository, i.e., the record's life cycle. Therefore, in this section, we discuss the record's life cycle. Based on this discussion, the requirements for evidential value will be specified in the next section.

The DCC (Digital Curation Centre) model the curation life cycle by different actions [23]. These actions fall into three groups, which are Full Life Cycle Actions, Sequential Actions and Occasional Actions. The Preservation Planning and Conceptualize actions in this model are used to determine the preservation strategy as well as to conceive and plan the creation of the record. These are not relevant with the record because they do nothing related to the record.

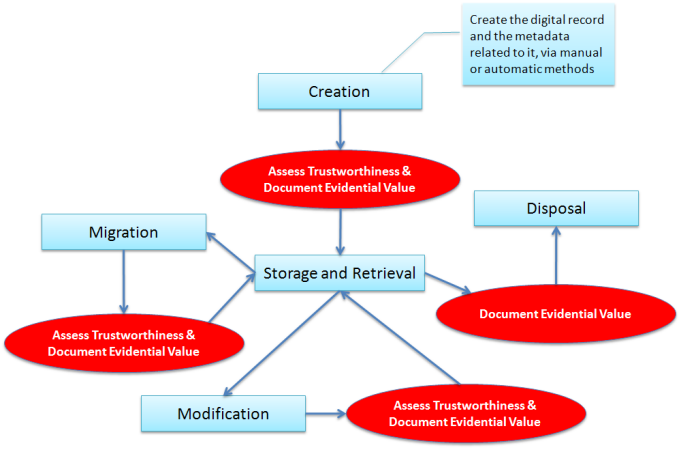

Fig. 3. The new record's life cycle.

Given that the record's life cycle model we want is specifically used to categorize the requirements for evidential value and it should concentrate on assessing the record's trustworthiness, it is reasonable to require that the desired life cycle model shall highlight the phases where the trustworthiness of the record might be changed. In other words, the phases which do not change the trustworthiness of records should be simplified. Based upon this requirement, the DCC life cycle model is not suitable.

The Government of South Australia proposed their model in 2006 [24], phases in this model are all relevant to the records. However, in this model, they do not distinguish modification and migration from preservation phase. Thus, according to the requirement for the life cycle model we stated above, this model is not very suitable for specifying the requirements for assessing the trustworthiness of records.

Since we cannot find a record's life cycle model which is perfectly suitable for being used to specify the trustworthiness requirements for evidential value, we propose our own record's life cycle model. In our model, we give much attention to those phases during which the trustworthiness of a record is likely to be compromised, and little attention to those phases during which the trustworthiness will not be compromised. As shown in Figure 3, there are six phases for the digital records stored in the archival repositories. These six phases are *creation*, *store*, *retrieval*, *modification*, *migration*, and *disposal*. Whenever the record needs to be preserved in digital repository, its trustworthiness has to be assessed and the related evidential value shall be documented and preserved.

A. Creation

The creation phase is the time when archival organizations receive documents (from both inside and outside) and create the corresponding records, as well as evidential value. The records and its related evidential value will later be preserved in digital repositories. As the ingest phase described in the OAIS model [1] and TRAC (Trustworthy Repositories Audit & Certification) project [2], in this phase, the repositories receive the records transferred to them, authenticate the source of all materials, and verify the completeness and correctness of these records. Given that we are focusing on research of the assessment of trustworthiness of digital records, the completeness and correctness of received records are not our concerns. We investigate what should be preserved as the evidential value, which could later be used to provide historical information to assess the records' trustworthiness.

B. Storage and Retrieval

After the records were created, they will be preserved in archival repositories, similar to the data management and preservation planning functions in OAIS model [1] and the preservation and store actions in DCC curation life cycle model [23]. Given that we need to distinguish the phases which might change the trustworthiness of records, we categorize the preservation stage into four phases in our model, i.e., store, retrieve, modify and migrate. In our research, we integrate store and retrieval, since they do not change the trustworthiness of records. The modification and migration are two separated phases as demonstrated below. The store and retrieval issues are currently being researched by the Find and Read work packages, respectively, in the LongRec project [5] (about the LongRec project and Trust work package, please refer to Section I). We will not elaborate the store and retrieval phases in archival repositories any further.

C. Modification

After the records are preserved in archival repositories, the contents of the records can still possibly be modified, defined as the modification phase in our model. For example, organization might have two trustworthy copies for one document, each copy consist of one or more records. If some content in one record (R1) of a copy is missing, while the corresponding record (R2) of another copy is not, then the missing content in R1 should be modified based upon the content in R2. Thus, even in the archival repositories which are intended to preserve the real history and do not accept any amendment, modification of the records' content is still possible. As proposed by Duranti and Blanchette [4] any changes to the record have to be documented for the need to attest the authenticity of it. In the modification phase, the data related to the modification, such as *person*, *time*, and *purpose* of the modification as well as what has been modified, shall be preserved in order to provide evidence and needed information for assessing the records' trustworthiness. In addition, Thomas et al. [25] stated that *"Evidence record must allow detection of any modifications to it and the appropriate data object."*. As we have defined above, the historical information in the evidential value includes the data related to the modification, and can be used to detect modifications to the archival records.

D. Migration

After working for some time, the archival repository will probably be migrated for various reasons, typically not enough space for storing additional records, or the digital formats used

currently will no longer be supported. Hence, the repository may be migrated from a smaller disk to a larger one (called *copy*), or it may be migrated from one digital format to another (called *conversion*), since the old format is to be abandoned. When doing conversion, records are actually being modified and therefore conversion can be considered similar to the modification phase. As stated by Thomas et al. [25] *"it must be possible to transfer data object and its evidence record from one service to another without losing evidence value"*, therefore when doing copy, information related to this process has to be preserved in order to provide evidence. This information, also as historical information, is stored in the evidential value.

E. Disposal

As defined in the DCC model [23], the disposal phase is used to dispose records which are no longer needed according to documented policies, guidance or legal requirements. Even when the records are intended to be deleted, they are typically transferred to another archive, repository, data centre or other custodian, where these records might be stored as newly created records and their trustworthiness might need to be assessed. Therefore, it is still necessary to preserve the information related to the disposal in the evidential value. Note that the disposed record will not be preserved in the original repository where it used to be, hence the trustworthiness assessment of this record is not necessary in the original repository, we only need to document and preserve the evidential value.

V. Requirements for Evidential Value

After we understand what evidential value is, why it is essential to assess the record's trustworthiness and how it can be categorized, we finally assess and specify the requirements for evidential value in this section. Given that we are focusing on the trustworthiness of the record in long-term preservation repository in this paper, we start with making the assumptions:

- The record we mention here is the digital record which is intended for long term usage.
- The access control of the repository has been satisfied. That means the person who might retrieve, modify and migrate the records is authorized, we will not deal with the security issues here.

Although the InterPARES project listed requirements of what evidence the preserver must obtain to support authenticity of electronic records in their book [26], their list do not show the details of these requirements. Therefore, we will elaborate the requirements for evidential value, which can be used to assess the records' trustworthiness.

A. Requirements during Creation

Pertaining to the creation process, information listed below should be stored as evidential value, in order to give sufficient information for trustworthiness assessment at a later time.

1) Information about Originator: Originator is the person who actually created the original content of a record. Since the record might be received from outside or created from paper form, the originator can be different from the creator of the record. It is necessary to document this information, because the trustworthiness of the content might be gained from the originator's identity. For example, certain experts can assess an artwork's trustworthiness by checking the author's style.

- Name of Originator (if available).
- Affiliation of Originator (if available).
- Compose Time (if available). The compose time is necessary for assessing the originator's style, since an originator's style can vary over time.

2) Information about Creator: The creator is the person who creates the digital records which is stored in the archival repository. It is obvious that the identity of the creator can be used to assess a record's trustworthiness, because the record created by a person outside might not be recognized as highly trustworthy.

- Name of Creator. The creator is not necessarily to be the originator as we explained above.
- Affiliation of Creator.

3) Information about Creation: As stated in the definition of evidential value, the information of a record creation shall be documented in order to provide evidences for the assessment of trustworthiness at a later time.

- Time of Creation. The date and time when the record was created. For example, a batch of records might be created together. If the time of creation of a record in that batch is much different from others, it should be recognized as lower trustworthiness than others, since this difference might be caused by a problem of the software or by somebody's tampering.
- Software Used for Creation. The software used for creation need to be documented, since the trustworthiness of the software can be evaluated. Created record might be recognized as lower trustworthiness, if it is created by software with low trustworthiness.
- Source of Record. The source of the records if they were transferred from outside or transformed from other forms or formats. E.g. it is reasonable to think that records transformed from internal is more trustworthy than records from other sources.
- Reason & Purpose. The reason and purpose for why the record was created, e.g. transform paper documents into digital records in order to archive the documents. The reason or purpose can give supplementary information for assessing the trustworthiness of the record.

B. Requirements during Storage and Retrieval

The storage and retrieval phases will not be elaborated because both of them will not alter the records and will not increase or decrease the trustworthiness of records. As we stated at the beginning of this section, the security issues, such as permission control, are not the topics of this paper.

C. Requirements during Modification

After records were archived, it is still possible to modify them. As demonstrated by several researchers [4], [25], a trusted archiving system should be able to detect any modifications to the records.

1) Information about Modifier: Like the creation phase, the identity of modifier is useful to trace the person and validate the modification action.

- Name of Modifier.
- Affiliation of Modifier.

2) Information about Modification: As stated in section IV-C, the historical information about the modification should be stored as evidential value. This information is:

- Time of Modification. The date and time when the modification has occurred. The modification happened in a rest time shall not be recognized as highly trustworthy.
- List of Originals. A list of all the original content in records which will be modified. This list shall be given before the modification.
- List of Modifications. A list of all the modified content in records which were modified. This list shall be given after the modification.
- Source for Modification. The source which the modification is based on. The source might be the corresponding record from another copy of the genuine data as in the example we mentioned in Section IV-C. It might also be the source which is used to create the records.
- Reason & Purpose. The reason and purpose for why the records need to be modified.

D. Requirements during Migration

Since the original records might be deleted after migration due to lack of disk space, it is necessary to have a person to verify the records after migration. Therefore, when doing migration, not only identity of the person who performs the migration needs to be stored, but also the person who verifies the migration.

1) Information about Migration Executor: Migration might be carried out by software programs, however, no matter which software program is used, there must be a person who actually starts the program. Hence, we used this information to identify the person to check his/her trustworthiness.

- Name of Person Who Executes Migration.
- Affiliation of this Person.

2) Information about Verifier: Similar to the migration executor, the person who verifies the migration shall be able to be identified, no matter he/she use verification program or not.

- Name of Verifier.
- Affiliation of Verifier.

3) Information about Migration & Verification:

- Time of Migration & Time of Verification. Both time of migration and time of verification can be used to see whether migration or verification is performed at working time, and therefore make the migrated records have lower or higher trustworthiness.
- Software used for Migration & Verification. The software used for migration and verification are documented, because the trustworthiness of the software can also be evaluated. Migration or verification might be considered to decrease the trustworthiness of records, if it is executed by software with low trustworthiness.
- Reason & Purpose. The reason and purpose are good complementary information for understanding why migration was carried out. This information can further help the assessment of records' trustworthiness.

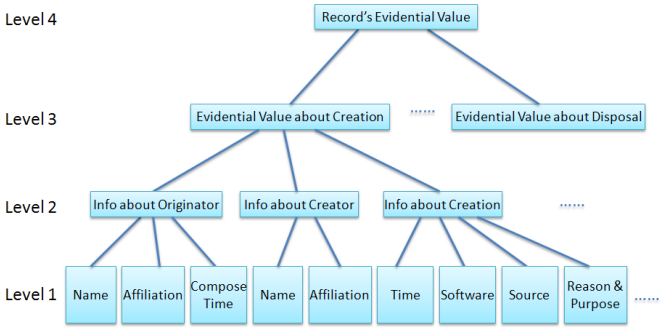

Fig. 4. The tree structure of a record's evidential value.

E. Requirements during Disposal

Even the records were chosen to be disposed, they might be transferred to another place instead of being deleted [23]. Therefore, as we have stated in section IV-E, the information of disposal shall be stored in evidential value. This information is about Disposal Executor and Disposal.

1) Information about Disposal Executor: The identity of the person who disposes the records shall be documented.

- Name of Disposal Executor.
- Affiliation of this Person.

2) Information about Disposal: Since the record might be transferred to another place instead of being deleted [23], the information of disposal has to be documented. The time and reason & purpose of disposal can show when and why the records are disposed.

- Time of Disposal.
- Reason & Purpose.

VI. Assessment of a Record's Trustworthiness Using Evidential Value

In this section, we briefly explain how the evidential value can be used to assess the trustworthiness of a record. We will develop the assessment method in our forthcoming papers.

After having elaborated the requirements for evidential value in Section V, we see that the record's evidential value can be structured as a tree model shown in Figure 4. For simplicity, we only draw sub-tree about evidential value about creation.

Figure 4 shows that the record's evidential value consists of evidential values from various phases of a record's life cycle. The evidential value in each phase is categorized by various perspectives, and each perspective is comprised of many attributes. The assessment of trustworthiness will start from the leaves of this tree (*level 1* as shown in Figure 4). Due to the differences of the origin and function of these leaves, a number of different linguistic values are assigned to each leaf. The linguistic values are typically described as very high trustworthiness, high trustworthiness, medium trustworthiness, low trustworthiness or no trust, and are used to express the degree of support of a certain "trustworthiness hypothesis". For example, the creator with name David might be assigned as very high trustworthiness since he is the person responsible for creating the record. These linguistic values will then be converted to numeric values from 0 to 1 at corresponding leaves. The numeric values are assigned as the mass function of these leaves, as defined in the Dempster-Shafer Theory [27]. The combination approach of the Dempster-Shafer Theory and the MADM method [28] can be used to combine the numeric values of these leaves into the nodes at *level 2*. The computed results are the degree of trust of the nodes at level 2, which will later be used to compute the degree of trust of the nodes at *level 3*. The combination process then continues to the highest level (*level 4*), and there we will get the assessed trustworthiness of the record, which is calculated by using evidential value.

VII. Conclusion and Future Work

In this paper, we have assessed the definitions of evidential value arrived at by other researchers before presenting our definition. By comparing trust in the real world with trust in the digital world, we illustrated how and why evidential value is essential in the assessment of the trustworthiness of a record. After discussing and assessing the life cycle models so far presented, we proposed a life cycle model which gives much attention to those phases during which the trustworthiness of a record is likely to be compromised, and little attention to those phases during which it will not be compromised. Based on this model we identified, analyzed and specified the requirements for evidential value at each phase, and explained briefly how these requirements can be used to assess the trustworthiness of a record in long-term storage.

Our conclusion is, therefore, that with an established rigorous set of requirements of evidential value, evidential value can be used for the reliable assessment and calculation of the degree of trustworthiness of a digital record over time.

In our future work we intend to include security requirements for evidential value since security supports the establishment of trust through the provision of secure and trustworthy environment, the validation of all requirements for evidential value by testing them in practical case studies and analyzing the results, and the development of methodology for the assessment and calculation of the degree of trustworthiness of a digital record based on evidential value.

References

[1] Consultative Committee for Space Data Systems, "Reference model for an open archival information system (OAIS)," National Aeronautics and Space Administration, Jun. 2001. [Online]. Available: http://ssdoo.gsfc.nasa.gov/nost/isoas/ref_model.html.

[2] Center for Research Libraries, "Trustworthy repositories audit & certification: Criteria and checklist," Jul. 2008. [Online]. Available: http://www.crl.edu/PDF/trac.pdf.

[3] S. Chokhani and C. Wallace, "Trusted archiving," in *Proceedings of the 3rd Annual PKI R&D Workshop*. NIST, Apr. 2004. [Online]. Available: http://middleware.internet2.edu/pki04/proceedings/trusted_archiving.pdf.

[4] L. Duranti and J.-F. Blanchette, "The authenticity of electronic records: The InterPARES approach," in *IS&T's 2004 Archiving Conference*, Apr. 2004, pp. 215–220. [Online]. Available: http://polaris.gseis.ucla.edu/blanchette/papers/ist2.pdf.

[5] LongRec, "Long-term record management." [Online]. Available: http://www.longrec.com/Pages/Default.aspx.

[6] N. Bartlett, "Applied research and teaching on archival appraisal," Jan. 2001. [Online]. Available: http://www-personal.umich.edu/~deromedi/module/nbdisc.htm.

[7] T. R. Schellenberg, *Modern Archives: Principles and Techniques*. University of Chicago Press, 1956.

[8] D. O. Stephens and R. C. Wallace, "Electronic records retention: Fourteen basic principles," pp. 1–10, Mar. 2001. [Online]. Available: http://archives.syr.edu/cnyarma/ARMAil0301.pdf.

[9] F. G. Ham, *Selecting and Appraising Archives and Manuscripts*, 1st ed. Society of American Archivists, 1993.

[10] T. R. Schellenberg, "The appraisal of modern public records," in *A Modern Archives Reader: Basic Readings on Archival Theory and Practice*, M. F. Daniels and T. Walch, Eds. National Archives Trust Fund Board, Aug. 1984, pp. 57–70.

[11] Pennsylvania Historical & Museum Commission, "Archival value of state government records." [Online]. Available: http://www.portal.state.pa.us/portal/server.pt?open=512&objID=3877&&PageID=494510&level=5&css=L5&mode=2&in_hi_userid=2&cached=true.

[12] UNC School of Information and Library Science, "Definitions — Managing the digital university desktop." [Online]. Available: http://ils.unc.edu/digitaldesktop/definitions.html\#evidential.

[13] University of Missouri System, "Electronic record management," Jan. 2007. [Online]. Available: http://www.umsystem.edu/ums/departments/fa/management/records/electronic/what.shtml.

[14] University of Toronto, "Glossary — University of toronto archives & records management services." [Online]. Available: http://www.library.utoronto.ca/utarms/info/glossary.html.

[15] Tennessee Archives Management Advisory, "Appraisal and disposition of records." [Online]. Available: http://www.tennessee.gov/tsla/aps/tama/tama01appraisal.pdf.

[16] M. K. Sitts, Ed., *Handbook for Digital Projects: A Management Tool for Preservation and Access*, 1st ed. Northeast Document Conservation Center, 2000. [Online]. Available: http://www.nedcc.org/resources/digitalhandbook/dman.pdf.

[17] Archives Working Group, "Acquisition policy for the james hardiman library archives." [Online]. Available: http://www.library.nuigalway.ie/export/sites/JHL/resources/archives/archives_docs_II/acquisition_policy.pdf.

[18] Arizona State Library, Archives and Public Records, "Evidential value — Arizona electronic records thesaurus," Nov. 2007. [Online]. Available: http://rpm.lib.az.us/alert/thesaurus/terms.asp?letter=e.

[19] BusinessDictionary, "Evidential value — Businessdictionary." [Online]. Available: http://www.businessdictionary.com/definition/evidential-value.html.

[20] J. M. Reitz, "Dictionary for library and information science," Nov. 2007. [Online]. Available: http://lu.com/odlis/odlis_a.cfm#archivalvalue.

[21] J. Ma, H. Abie, and T. Skramstad, "Preservation of trust and security in long-term record management," Oct. 2008, Fredericton, New Brunswick, Canada.

[22] Wikipedia, "Metadata — Wikipedia, the free encyclopedia," 2009. [Online]. Available: http://en.wikipedia.org/wiki/Metadata.

[23] S. Higgins, "The DCC curation lifecycle model," *International Journal of Digital Curation*, vol. 3, no. 1, pp. 130–140, Jun. 2008.

[24] Government of South Australia, "Records life cycle," Jul. 2006. [Online]. Available: http://www.decs.sa.gov.au/rmp/pages/cg0000941/17694/.

[25] Thomas Kunz, Susanne Okunick, and U. Viebeg, "Long-term security for signed documents: Services, protocols, and data structures," 2009. [Online]. Available: http://www.dzi.tu-darmstadt.de/fileadmin/content/veranstaltungen/20060606-09_etrics/kunz_okunick_viebeg.pdf.

[26] L. Duranti, Ed., *The Long-term Preservation of Authentic Electronic Records: Findings of The InterPARES Project*, 2005.

[27] G. Shafer, *A Mathematical Theory of Evidence*. Princeton University Press, 1976.

[28] J.-B. Yang and M. G. Singh, "An evidential reasoning approach for multiple attribute decision making with uncertainty," *IEEE Transactions on Systems, Man and Cybernetics*, vol. 24, no. 1, pp. 1–18, Jan. 1994.