Addressing Privacy and Trust Issues in Cultural Heritage Modelling

Michalis Pavlidis[1], Haralambos Mouratidis[1], Cesar Gonzalez-Perez[2], and Christos Kalloniatis[3]

[1] University of Brighton
[2] Institute of Heritage Sciences (Incipit), Spanish National Research Council (CSIC)
[3] Cultural Informatics Laboratory, Department of Cultural Technology and, Communication University of the Aegean
{m.pavlidis,h.mouratidis}@brighton.ac.uk
cesar.gonzalez-perez@incipit.csic.es
chkallon@aegean.gr

Abstract. The management of cultural heritage information is an important aspect of human society since it enables us to document and understand our past and learn from it. Recent developments in ICT have significantly boosted research and development activities aimed at the creation and management of cultural heritage resources. As a result, information systems play an increasingly important role on storing and managing cultural heritage information and allowing preservation of the information in a digital way. To support such effort, a number of cultural heritage conceptual models have been developed and presented in the literature. However, such models they focus on the heritage entities and information, but fail to include issues such as privacy and trust. Our research has shown that these are important issues to consider in order to have a complete cultural heritage model. This paper presents the first work in the literature to include privacy and trust as part of a cultural heritage conceptual model. We demonstrate the applicability of our work using a real world case study from the Iron Age settlement of Castrolandin in Spain.

Keywords: Cultural Heritage, Information Systems, Privacy, Trust

1 Introduction

Heritage is anything that can be considered important to be passed to future generations and it is broadly divided into natural heritage and cultural heritage. Anything to which a social group attributes particular aesthetic, artistic, documentary, environmental, historic, scientific, social or spiritual values is commonly designated cultural heritage. Cultural heritage consists of tangible and intangible elements. Tangible elements include heritage sites, buildings and artefacts, while intangible elements include practices, representations, expressions, knowledge, and skills, or in other words elements that are embodied in people rather than in inanimate objects.

The management of cultural heritage information is an important aspect of human society since it enables us to document and understand our past and learn from it. Appropriate management is required for the effective identification, interpretation, maintenance, and preservation of significant cultural entities. It requires though having a deep and shared understanding of what cultural heritage is and what cultural heritage is composed of. Recent developments in ICT have significantly boosted research and development activities aimed at the creation and management of cultural heritage resources. As a result, information systems play an increasingly important role on storing and managing cultural heritage information and allowing preservation of the information in a digital way [1]. Having the information digitised also helps to make the information available on ways that was not possible before. For example, a number of archeological sites can be "visited" from anywhere in the world and visitors can view and receive information about artefacts like they are visiting the physical sites. However, this situation apart from the obvious advantages, introduces some privacy and trust issues. For example, part of digitised cultural heritage information may be private [2], and even though information might be personalised [3], still there have to be safeguards that will ensure there is no privacy violation.

On the other hand, many heritage entities, such as buildings, are tied to the land, which can be private property, and even some heritage entities are private property themselves. Local communities are fighting to preserve their way of life as part of their heritage. Travel and cultural institutions use this uniqueness to promote travel and tourism, and while this brings in revenue and exposure, cultural heritage sites that were preserved by virtue of their isolation are now being severely damaged and even destroyed. This situation introduces a wide range of cases where privacy issues must be respected by government organisations related to cultural heritage and other involved parties. For example, in some scenarios, the government can force the owner of a highly rated cultural heritage house to open it to the public a few days a month. However, this can result in a violation of the owner's privacy. Therefore, modelling explicitly the privacy requirements of such situations can contribute to the resolution of the aforementioned issues. Elements to model would include the details of privacy, what information is subject to what privacy levels, and who has access to what. In order to achieve this, it would be necessary to identify what actions must be carried out in order to protect the owners' privacy when cultural heritage entities are documented.

However, accomplishing this does not solve the uncertainty about whether the aforementioned actions related to privacy protection will be carried out or not. Without further analysis, they are just assumptions which may prove wrong and lead to violation of cultural heritage owner's privacy. The same situation exists when actions regarding the conservation and allowance of use of cultural heritage objects are considered. Such actions are assigned to agents but without further justification of whether the agents can be trusted to take them, they remain just assumptions. If the agents never realise the assigned actions, this will lead to a deterioration of the condition of the cultural heritage entity or

inconvenience it. Therefore, further analysis is required in order to justify if the agents assigned with certain actions can be trusted to do so, or that there are appropriate control mechanisms in place to ensure that the agents will do so.

To address these issues this paper presents a conceptual modelling approach that makes use of works from the fields of cultural heritage, privacy, and trust. CHARM [4, 5], PriS [6–8], and JTrust (Justifying Trust) [9, 10], respectively, are adapted and combined in a single conceptual model to jointly address this problem area. The next section provides background about these three approaches. Section 3 presents our proposed conceptual model while Section 4 presents a methodological process for using the conceptual model. Section 5 demonstrates the applicability and usefulness of our proposed model using a case study. Section 6 discusses the related work, followed by the conclusion and future work.

2 Background Information

The Cultural Heritage Abstract Reference Model (CHARM) [4, 5] is a wide and shallow conceptual model for cultural heritage, which includes over 160 classes representing very abstract concepts, such as Place, Material Entity, Agent, and Performative Entity. CHARM does not only represent the specific entities that might make up cultural heritage, but also other entities, which are necessary in order to describe and understand the former, such as documents, representations, and valorisations. These are the three major concerns that are captured in CHARM:

- Evaluable entities. An valuable entity is anything to which cultural value can be assigned. In other words, an evaluable entity is each of the individual things to which people can add cultural value. Evaluable entities comprise all the raw matter that may become cultural heritage, including tangible and intangible things.
- Valorisations. A valorisation is the discourse that adds cultural value to an evaluable entity. In other words, a valuation is the social and cultural vehicle that people use in order to produce cultural value.
- Representations. A representation is a persistent expression of one or multiple evaluable entities or valorisations.

The PriS method [6–8] is a requirement engineering methodology that incorporates the modelling and analysis of privacy requirements into the system development process. Privacy requirements are identified after the investigation of the implications that privacy goals have on ordinary organisational goals. PriS specifies the following eight privacy goals:

- Authentication
- Authorisation
- Identification
- Data Protection
- Anonymity

– Pseudonymity
– Unlinkability
– Unobservability

Furthermore, PriS specifies a set of rules to transform privacy requirements into implementation techniques through the use of privacy process patterns used for identifying system architectures, which support the privacy requirements.

JTrust [9, 10] is a methodology for reasoning about trust relationships and it is founded upon the notions of trust and control as the means of confidence achievement. Any dependency on entities of an information system to carry out an action introduces an uncertainty about the fulfilment of that dependency. It can also constitute a vulnerability for the system in case the other entity does not behave as expected, i.e. fulfil the dependency. Therefore, appropriate ways of removing the uncertainties and building confidence in the dependences is accomplished with the identification of dependency resolutions. Such resolutions need to be found based on trust or/and control. Moreover, in case of trust there four types of trust resolution:

– Experiential trust
– Reported trust
– Normative trust
– External trust

JTrust provides a structured way of identifying explicitly trust assumptions that underlie the system analysis and can endanger the satisfaction of the system requirements.

3   Cultural Heritage Conceptual Model with Trust and Privacy

A conceptual model can be described as an abstraction of reality according to a certain conceptualisation. This abstraction usually consists of an abstract representation of specific aspects of domain entities, called concepts. When a conceptual model is represented as a concrete artefact, it facilitates the communication and analysis of important and relevant aspects of the domain concerned. A conceptual model often serves as vehicle for reasoning and problem solving as well as for acquiring new knowledge about a domain. To be able for someone to use it, the conceptualisation should be expressed in a specific representation, such as a modelling language. The expression must be unambiguous and help users solve real world problems.

The proposed model combines concepts from the areas of cultural heritage, privacy, and trust. It can be used by software engineers when analysing or designing a cultural heritage information system. It enables them to capture information about the rights and obligations that agents have in relation to certain cultural heritage entities. It also enables them to capture privacy requirements related to obligations to allow the use or conserve a cultural heritage entity. Finally, it enables them to reason whether the agents assigned with privacy goals

can be trusted to satisfy them. In cases where there is lack of trust, control mechanisms can be identified in order to fill in the gap and provide the necessary confidence in the fulfilment of the assigned privacy goals. Our combined model is depicted in Figure 1. In the remaining section we describe its concepts, which are illustrated by using the following scenario.

An important aspect of cultural heritage are buildings that belong to a cultural heritage site. These buildings many times have an owner and a conservator who are different entities. The European Confederation of Conservator-Restorers' Organisations has issued a code of ethics. Article 3 states that the conservator-restorer works directly on cultural heritage and is personally responsible directly to the owner, to the heritage, and to the society. The conservator-restorer is entitled to practices without hindrance to her/his liberty and independence. Also, Article 18 states that the conservator-restorer is bound by professional confidentiality. In order to make a reference to an identifiable part of the cultural heritage she should obtain the consent of its owner or legal custodian. During the development of a conceptual model for such a scenario not only the cultural heritage aspects of the scenario have to be represented in the model, but also aspects that are related with the privacy of sensitive information and the trust relationships that affect the soundness of the model.

The following concepts have been adopted from CHARM:

An **Agent** is a primary entity corresponding to a person or group of people [11]. So, using the running example the owner of the building that constitutes cultural heritage is an agent and the conservator of the building is another agent.

An **Evaluable Entity** is an entity that has been, is or may be culturally evaluated [11]. The building that has a cultural heritage value is an evaluable entity in our running example.

A **Normative Situation** is an abstract entity corresponding to a right or obligation that one or more agents have, possibly in relation to a set of evaluable entities [11]. In the running example there are two normative situations that can be identified. First, the owner of the building has a right of ownership over it, and secondly, the conservator has the obligation to conserve the building in a good state.

A **Right** is a normative situation that provides its owners with specific liberties, guarantees or benefits, usually about certain evaluable entities [11]. In our conceptual model there are three types of rights, adopted from CHARM:

- A Right of Ownership is the right that provides its onwner with the benefit of owning the associated evaluable entities.
- A Right of Use is the right that provides its owner with the benefit of being able to use the associated evaluable entities.
- A Right of Custody is the right that provides its owner with the benefit of keeping the associated evaluable entities in their possession.

An **Obligation** is a normative situation that subjects its owners to specific obligations, usually in relation to certain evaluable entities [11]. In our conceptual model there are two types of obligation, adopted from CHARM:
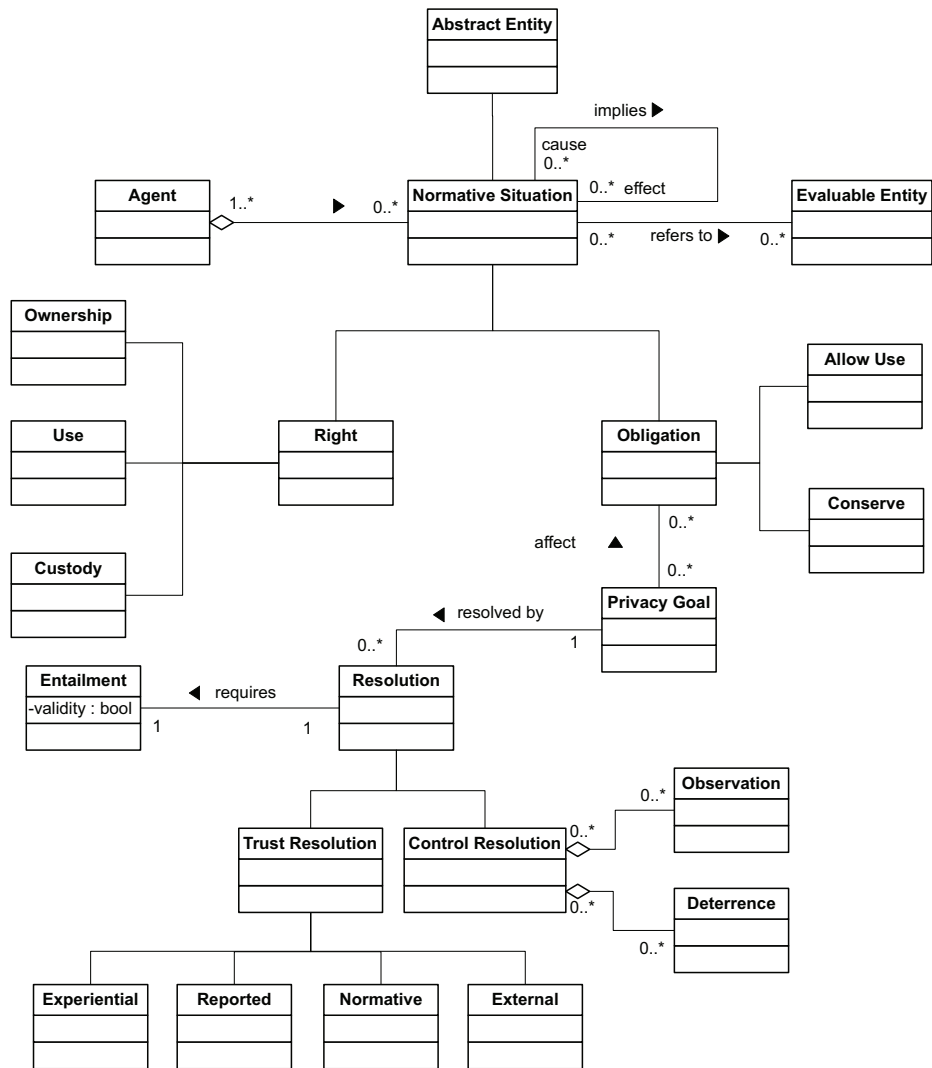
Fig. 1. Cultural heritage conceptual model with privacy and trust.

– An Obligation to Conserve is the obligation that requires its owner to keep the associated evaluable entities in good condition.
– An Obligation to Allow Use is the obligation that requires its owner to allow the use of the associated evaluable entities to certain third parties.

A **Privacy Goal** expresses a privacy requirement which constraints the casual transformation of organisational goals into processes [6–8]. If a goal is assigned to an agent then this means that she has to make some adjustments in the processes that implement the organisational goals that are affected by the privacy goal. As mentioned in the previous section eight type of privacy goals are recognised: identification; authentication; authorisation; data protection; anonymity; pseudonymity; unlinkability; and unobservability. Privacy goals affect obligations and, therefore, in our running example the obligation of the conservator to conserve the cultural heritage building is affected by a data protection privacy goal as there are certain regulations that the conservator must comply with when handling private information. In particular, the conservator must not disclose any information that can be used to link related information about the owner. Also, the conservator must not disclose any identifiable information about the owner of the building. In order to make a reference to an identifiable part of the cultural heritage she should obtain the consent of its owner.

A **Resolution** is the way the uncertainty of the dependency on an agent is removed and confidence in the fulfilment of privacy goals is achieved [9]. In our running example, we assume that there is no control over the conservator company and we have confidence that it will handle the private data according to the relevant regulation because we trust it to do so. Therefore, there is trust resolution.

A **Trust Resolution** is the situation where confidence in the agent is achieved because of trust in the agent[9]. Four types of trust resolution are identified:

– Experiential trust is trust in the agent that originates from previous direct experience with the agent. If there was experiential trust resolution in our running example then this means that there is previous direct experience with the conservator and that is why we have confidence that it will fulfil its assigned privacy goal.
– Reported trust is trust in the agent that originates from a third party, the reporter. In a similar way, is a third party was reporting that the conservator will fulfil its privacy goal then we have confidence because of reported trust resolution.
– Normative trust is trust in the agent that originates from the system environment norms. If the conservator was a well established company in its field that everyone trusts it to respect and fulfil its privacy goal then we have confidence in the fulfilment of the goal because of normative trust resolution.
– External Trust is trust in the agent that originates from sources outside of the system environment. If there was an agent outside of the system environment that was suggesting us that the conservator will fulfil the privacy goal then

we have confidence in the fulfilment of the goal because of normative trust resolution.

A **Control Resolution** is the situation where confidence in the agent is achieved because of the agent being controlled [9]. Control is the power that one agent has over another agent to influence its behaviour and consists of two mechanisms: observation and deterrence.

An **Observation** is the measure through which an agent's actions are monitored. Therefore, in the running example if we wanted the conservator to be controlled then we could have assigned another company to monitor and audit its processes and verify that it is complying with the relevant regulations concerning data protection.

A **Deterrence** is the measure through which a agent is prevented from accomplishing one of her own goals. Observation alone is not adequate in order control to be effective. Somehow, there has to be a way to prevent the controlled agent from accomplishing her own goals in order to have an incentive to show the desired behaviour. In the running example, a mechanism of deterrence could be the termination of the contract, in case we observe that the conservator does not comply with the relevant regulations. That will prevent the conservator from accomplishing one of its own goals, which is to get paid and provide the incentive to show the desired behaviour.

An **Entailment** is a condition of trust. It originates from a dependency through the identification of a dependency resolution. Entailments are required to be valid in order to have confidence in the dependencies from which they originated [9]. Every resolution can lead to an entailment, for example reported trust has an entailment that the reporter can be trusted for what is reporting. Such entailments have to be validated by collecting evidence, otherwise there is no confidence in the fulfilment of the dependency. In the running example, the dependency on the conservator is resolved through normative trust that has the entailment that the system norm can be trusted. Consequently, evidence has to be collected, perhaps through surveys, in order to prove that the entailment is valid.

4   Methodological Process

In this section, we propose a methodological process by which the conceptual model presented in the previous section can be applied. The process consist of five activities and is depicted in Figure 2.

- **Identify normative situations between agents and evaluable entities.** The modeller identifies the relevant evaluable entities. Also, the agents that are related to them through with some kind of normative situation, as well as the type of normative situations themselves, have to be identified.
- **Privacy goal identification.** The modeller investigates the privacy issues that arise from the interconnected normative situations and models the privacy goals that affect the normative situations. Privacy goals can also be identified directly from respective legislation or directives.
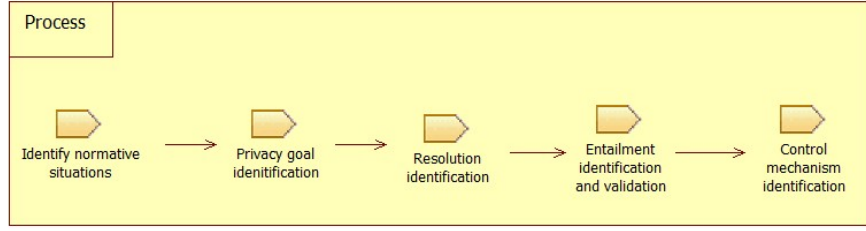
Fig. 2. Proposed process.

– **Resolution identification.** Even though privacy goals have been defined and have been assigned to appropriate agents, this is still not sufficient, because there is uncertainty on whether these agents will behave as expected and fulfil their responsibilities. In order to remove the uncertainty, specific resolutions of dependencies on these agents have to be identified. The resolutions can be trust resolutions or control resolutions.

– **Entailment identification.** Having identified the resolutions, the next step is to identify the entailments, which essentially are trust assumptions. These have to be validated based on evidence that has to be collected. Evidence can be collected with the use of surveys, interviews with the stakeholders or investigation of historical data.

– **Control mechanism identification.** Not all entailments are valid and therefore, further actions are required. Control mechanisms need to be identified and put in place in order to build confidence that the assigned privacy goals will be fulfilled. The technical system or another agent need to act as the controllers who will drive the agents to show the expected behaviour. To this end, the modeller must identify the necessary observation and deterrence measures.

5 Case Study

In this section we describe a case study that was used to examine the applicability of the proposed approach. The case study is based on an actual cultural heritage place, the Iron Age settlement of Castrolandin, located in Galicia (North-West Spain), where a series of research and public presentation projects have been carried out in the last few years [12]. The site consists of a series of ramparts and ditches on a hilltop, conforming a typical Iron Age hill fort, regionally know as a 'castro'. It had been known and described since the mid 20$^{\text{th}}$ century by archaeologists and was finally included in the official inventory of heritage sites following the usual procedure. An archaeological consultancy was hired by the regional government for the recording of heritage sites within the region. A record log was assigned to the site as a heritage place and a series of land use regulation were imposed to the area designated as its extent.

Moreover, another research project was developed on the site aimed at the anthropological documentation of the local community's perceptions and feelings about the site. This project allowed for the description and study of a traditional feast, nowadays lost, that had occurred on the site at least between the late 19th and mid-20th centuries. Descriptions of the feast of San Xoan (St. John's) are known thanks both to some written records and the memories of local elderly people. Thanks to this project, the feast of San Xoan was brought back to life in 2003, and repeated since on an annual basis. As a result the regional government extended the area that was subject to heritage protection and land use restrictions, and also declared the feast of San Xoan as a protected intangible heritage element

As a result of the generated archaeological, anthropological, and historical knowledge about Castrolandin, the regional government decided to intervene in order to apply the necessary protection schemes on both the site and the San Xoan celebration itself. The first scheme is called "Place of Cultural Interest" (BIC) and the second scheme "Celebration of Cultural Interest" (FIC), which is mainly applied to intangible entities. According to BIC, the owners of objects of cultural interest are obliged to facilitate their inspection by approved bodies, their study by researchers, and public entry at least four days a month and for movable objects to place them in a suitable position for viewing for a period of at least five months every two years [13].

In order all this information to be accessible to the public through an information system, it has to be organised and documented. However, such information contains private data that has to be kept confidential, such as the manifestation of the celebration every year that includes the private data of the individuals who have attended the San Xoan and the valorisation of the celebration that includes private data of the local elderly people. Therefore the private data has to remain confidential.

An information system that has to provide information about the cultural heritage of Castrolandin will be best designed at the conceptual level and will also facilitate better communication between the software engineers of the system and the stakeholders. This conceptual model has to consider not only the cultural heritage aspects of the information, but also the privacy and trust issues that are equally important for the stakeholders. The system development process will significantly benefit by being informed from such a conceptual model.

Next, the activities described in the previous section are applied to the case study of Castrolandin in order to demonstrate how to apply the proposed conceptual model and the developed model is depicted in figure 3.

Identify normative situations between agents and evaluable entities.
In our case the evaluable entities, i.e. the entities that can have a cultural heritage value, are the Castrolandin hill fort and the celebration of San Xoan. On the other hand, the agents in the case study are the regional government, the local citizens of the area, the conservator of the Castrolandin hill fort, and the visitors that may desire to seek information about the site and the surrounding area. The

visitors can be individuals who physically visit the site and the celebration, or visitors of a website who browse information about the site and the celebration. Having identified the evaluable entities and the agents involved, the following normative situations are identified through discussions with the agents and other stakeholders, and by inspecting the relevant laws.

i) The regional government has the right of ownership of the San Xoan celebration.
ii) The local citizens have the right of custody of the San Xoan celebration.
iii) The visitors have the right to use the San Xoan celebration.
iv) The regional government has the obligation to allow use of the San Xoan celebration.
v) The regional government has the right of ownership of the Castrolandin hill fort.
vi) The visitors have the right to use Castrolandin hill fort.
vii) The regional government has the obligation to allow use of the Castrolandin hill fort.
viii) The conservator has the obligation to conserve the Castrolandin hill fort.

Privacy Goal Identification. This activity aims at identifying the privacy goals that affect the normative situations identified in the previous activity. The first issue is with the organisation of the San Xoan celebration where the local citizens who are attending the celebration and want their private information to be kept anonymised. Furthermore, the conservator who has the obligation to conserve the Castrolandin hill fort is required to comply with the privacy regulations regarding the processing of personal data. Therefore, the respective privacy goals are incorporated into the conceptual model as shown in Figure 3. There are two privacy goals. The fist one is to ensure the anonymity of the participants of the San Xoan celebration and it is assigned to the regional government. The second privacy goal is to ensure data protection when conserving the Castrolandin site and it is assigned to the conservator. In effect, the regional government and the conservator need to take appropriate actions in order to ensure the satisfaction of the identified privacy goals.

Resolution Identification The dependencies though on the regional government and the conservator introduce an uncertainty on whether they will behave as expected, i.e. take actions in order to ensure the satisfaction of the privacy goals. To this end, resolutions of the two dependencies need to be identified that show the reasoning behind the removal of the uncertainty and the establishment of confidence in the fulfilment of the dependencies. The dependency on the regional government to hold the attendees anonymous is resolved with experiential trust. This means that the software engineer has previous direct experience with the regional government because of previous collaboration in other projects and believes that the regional government can be trusted to satisfy the privacy goal. The dependency on the conservator to comply with the relevant data protection

laws is resolved with reported trust. The company of the software engineer has a business partner, who reports to her through discussions that the conservator will comply with the data protection regulations.

Entailment Identification. The identified resolutions of the previous activity can systematically reveal the explicit trust assumptions underlying the developed conceptual model. We call such assumption entailments of resolutions, which have to be valid otherwise the analysis made in order to construct the model is not justified. The experiential trust resolution of the dependency on the regional government requires an entailment that the software engineer can trust herself for that decision. The reported trust resolution of the dependency on the conservator requires and entailment that the business partner, who acts as a reporter, can be trusted for what it is reporting. After the identification of entailments, evidence is gathered in order to decide whether the entailments are valid. There is substantial evidence from previous direct experience with the regional government, such as documents, which show that the regional government was indeed carrying out actions in the past to satisfy the anonymity related privacy goal and therefore that it can be trusted to satisfy it in this case as well. On the contrary, there was no enough evidence that the business partner can be trusted for what it is reporting, i.e. the conservator will fulfil the data protection privacy goal assigned to her. Consequently, the uncertainty regarding the fulfilment of the data protection related privacy goal by the conservator still remains.

Control Mechanisms Identification. As long as there is no justification regarding the fulfilment of the second privacy goal then the developed model cannot be qualified as sound in terms of preserving the privacy of personal information. Further actions are required in order to gain confidence in the fulfilment of the privacy goal by the conservator. As a solution a new control resolution was added as shown in Figure 3. It contains as an observation mechanism that the conservator will be audited periodically, and as a deterrence mechanism that the contract will terminate instantly in case she does not fulfil the privacy goal. This control resolution provides us the necessary confidence that the privacy goal will be fulfilled.

6   Related Work

The literature provides a number of approaches that support conceptual representation of cultural heritage. However, to the best of our knowledge, there is no work in the literature that incorporates privacy and trust modelling and analysis in such conceptual frameworks.

CIDOC CRM [14, 15] is a core ontology to enable information integration for cultural heritage data and their correlation with library and archive information. It was developed empirically by an interdisciplinary team, based on
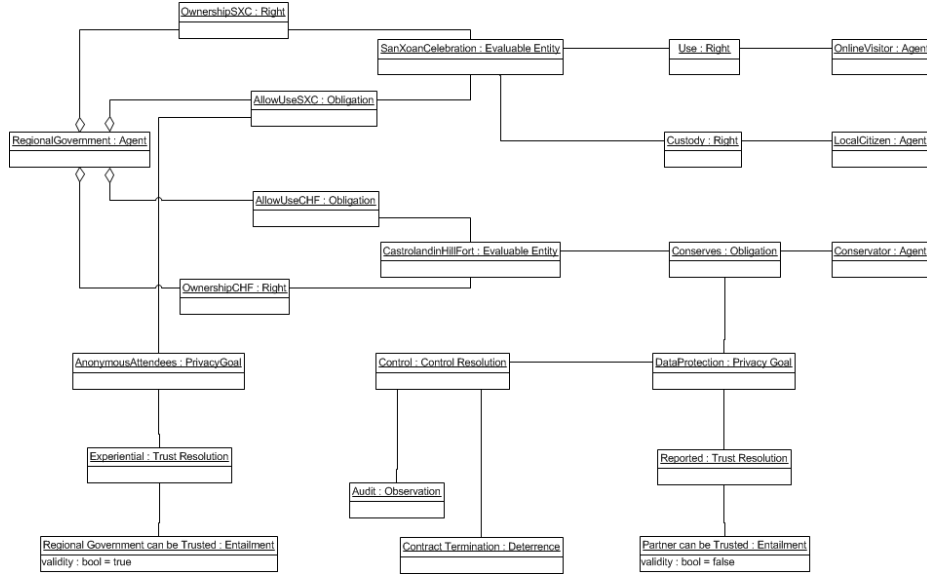
Fig. 3. Castrolandin site cultural heritage conceptual model.

real world cultural heritage information sources and may be used for analysing and designing cultural information systems. CIDOC CRM, ISO 21127:2006 [15, 16] is a standard for knowledge sharing in cultural heritage. The FRBR model [17], which was initially intended as a conceptual framework for bibliographic data, but the report gives a detailed description of entities, relationships and attributes that may be used to define type-vocabularies. The Dublin Core [18] is a flexible and usable metadata schema enabling information exchange and integration between digital sources. It is widely used by almost all digital libraries since it is simple, small and easily expandable, providing qualifiers enabling the semantic expression. The authors in [19] propose a Cultural Heritage application schema that enables the structured representation of natural sites that have been evaluated as cultural heritage.

7 Conclusion and Future Work

This paper has argued the need to incorporate privacy and trust into cultural heritage conceptual models, and it has presented the first conceptual model in the literature to include trust and privacy. Our work builds on approaches from cultural heritage, privacy, and trust conceptual modelling, and it combines them to develop a unified approach. A real cultural heritage case study from the area of Castrolandin in Spain, which has be characterised as cultural heritage site, has been employed in order to demonstrate the applicability of our work. We plan to apply our work to more case studies to enable us to increase the applicability of our approach.

References

1. Doerr, M.: Ontologies for cultural heritage. In: Handbook on Ontologies. Springer (2009) 463–486
2. Garzotto, F., Salmon, T., Pigozzi, M.: Designing multi-channel web frameworks for cultural tourism applications: The muse case study. (2003)
3. Ardissono, L., Kuflik, T., Petrelli, D.: Personalization in cultural heritage: the road travelled and the one ahead. User modeling and user-adapted interaction **22**(1-2) (2012) 73–99
4. Gonzalez-Perez, C., Parcero-Oubiña, C.: A conceptual model for cultural heritage definition and motivation. In: Revive the Past: Proceeding of the 39th Conference on Computer Applications and Quantitative Methods in Archaeology, Amsterdam University Press. Beijing (China) (2011) 234–244
5. Gonzalez-Perez, C.: Charm white paper, version 1.0.3. Technical report (2015)
6. Kalloniatis, C., Kavakli, E., Gritzalis, S.: Addressing privacy requirements in system design: the pris method. Requirements Engineering **13**(3) (2008) 241–255
7. Kalloniatis, C., Kavakli, E., Gritzalis, S.: Pris methodology: incorporating privacy requirements into the system design process. In: Proceedings of the SREIS 2005 13th IEEE International Requirements Engineering Conference–Symposium on Requirements Engineering for Information Security. (2005)
8. Kalloniatis, C., Kavakli, E.: Pris tool: A case tool for privacy-oriented requirements engineering. In: Proceedings of the MCIS 2009 4th Mediterranean Conference on Information Systems G. Doukidis et al. (Eds.). (2009) 913–925
9. Pavlidis, M., Islam, S., Mouratidis, H., Kearney, P.: Modeling trust relationships for developing trustworthy information systems. International Journal of Information System Modeling and Design (IJISMD) **5**(1) (2014) 25–48
10. Pavlidis, M., Mouratidis, H., Islam, S., Kearney, P.: Dealing with trust and control: A meta-model for trustworthy information systems development. In: Sixth International Conference on Research Challenges in Information Science (RCIS). (May 2012) 1–9
11. Incipit: CHARM Online Reference, version 0.9.0.1. (accessed February 3, 2015)
12. Ayán Vila, X., et al.: Pasado e futuro de castrolandín (cuntis): Unha proposta de recuperación e revaloración. (2002)
13. Howard, P., Ashworth, G.: European Heritage, Planning and Management. Intellect Books (1999)
14. Doerr, M.: The cidoc conceptual reference module: an ontological approach to semantic interoperability of metadata. AI magazine **24**(3) (2003) 75
15. Doerr, M., Hunter, J., Lagoze, C.: Towards a core ontology for information integration. Journal of Digital information **4**(1) (2006)
16. Doerr, M., Ore, C.E., Stead, S.: The cidoc conceptual reference model: a new standard for knowledge sharing. In: Tutorials, posters, panels and industrial contributions at the 26th international conference on Conceptual modeling-Volume 83, Australian Computer Society, Inc. (2007) 51–56
17. Maxwell, R.L.: FRBR. ALA Editions (2007)
18. Weibel, S.L., Koch, T.: The Dublin Core metadata initiative. D-lib magazine **6**(12) (2000) 1082–9873
19. Fernández Freire, C., Pérez Asensio, E., Bosque González, I.d., Uriarte González, A., Vicent García, J.M., Fraguas Bravo, A., Parcero-Oubiña, C., Fábrega-Álvarez, P., et al.: Proposal for a cultural heritage application schema within the INSPIRE directive. (2012)