Pers Ubiquit Comput
DOI 10.1007/s00779-009-0233-8

ORIGINAL ARTICLE

Context-based authentication and transport of cultural assets

Leonardo Mostarda · Changyu Dong · Naranker Dulay

Received: 2 December 2008 / Accepted: 9 March 2009

Abstract We present a ubiquitous system that combines context information, security mechanisms and a transport infrastructure to provide authentication and secure transport of works of art. Authentication is provided for both auctions and exhibitions, where users can use their own mobile devices to authenticate works of art. Transport is provided by a secure protocol that makes use of position–time information and wireless sensors providing context information. The system has been used in several real case studies in the context of the CUSPIS project and continues to be used as a commercial product for the transportation and exhibition of cultural assets in Italy.

Keywords Ubiquitous systems · Authentication

1 Introduction

Exhibitions and auctions make a substantial contribution to the world economy. In 2006, 2,000 national museums, monuments, archaeological sites and exhibitions in Italy and France were visited by 54 million people with an average fee of 6.3 € per person [2]. In the same year the Artprice reports an annual auction sales turnover of 5 billion euros [3]. Such a profitable market has drawn the attention of criminal organisations that have started to fake and steal works of art. Current trade in counterfeit and stolen artworks is a six billion US dollars per year business and the largest crime in the world after drug and gun trafficking [4]. For instance, some people have paid 50,000 to buy fake Picasso, Miro and Dali paintings sold in exhibitions and auctions [3]. Counterfeit cultural assets have been used to attract people to exhibitions and boost the sale of exhibition tickets. Even with good planning and the presence of security agencies, criminals are still able to steal works of art during transport [5].

Existing solutions are often inadequate to address the problems. To prevent counterfeiting, paper certificates are used. A certified organisation checks the provenance, the style of the artist, and uses forensic methods (e.g. carbon dating [6], thermoluminescence [7] and statistical analysis of digital images [8]) to verify the artwork's authenticity. If the asset is authentic, the organisation signs a paper certificate containing artwork details. The problem with paper certificates is that they can easily be forged or duplicated and then presented with counterfeit works of art. During transport, criminals are still able to steal works of art [5]. This happens most often when asset delivery is carried out by several transportation operators.

To address the aforementioned problems we develop a secure context-aware system. The system utilises position and time information and provides security protection throughout the cultural asset life cycle. The protection can be divided into four phases: certification, identification, transport and authentication of artwork.

In the certification phase organisations that claim to be qualified for asset authentication, for example a museum, interact with a government authority in order to obtain a

This article is a revised and extended version of a paper that was presented at the IFIPTM 2008 conference [1].

L. Mostarda (✉) · C. Dong · N. Dulay
Department of Computing, Imperial College London, London SW7 2AZ, UK
e-mail: lmostard@doc.ic.ac.uk

C. Dong
e-mail: cd04@doc.ic.ac.uk

N. Dulay
e-mail: nd@doc.ic.ac.uk

Published online: 21 April 2009

digital qualification (certificate). In the identification phase our system assigns a tag to each cultural asset identifying the place where, and the time when, the artwork is to be sold/exhibited, as well as a description of it, for example, text or a picture signed by an organisation. In the transport phase, a context-aware service is used to provide secure transport. We use a positioning system to ensure the lorry follows the right path at the right time, and we use sensor readings (distance, temperature, light and humidity) to detect package tampering.

During transport, any entity that tries to open the package is detected unless it is authorised and the right destination has been reached. In the authentication phase users can use their own mobile devices to perform an off-line tag verification process. This process ensures that, although a valid tag can still be copied by an adversary, its use in a different position and time is detectable. The authentication approach is independent from the object tagging technology (e.g. shotCode and RFID) and can work with several definitions of context as long as the context is uniquely authenticated.

The system was implemented as part of the CUSPIS European project and validated on real case studies [9]. It has also been integrated with a ubiquitous virtual guide that provides information inside museums and auctions.

The article is organised as follows. In Sect. 2, we describe the scenarios, the threat model and the system requirements. In Sect. 3, we describe the protection provided throughout the cultural asset life cycle. In particular, Sects. 3.1 and 3.2 describe the certification and identification phases, Sect. 3.3 describes our context-aware transport protocol, Sect. 3.4 shows the authentication phase and Sect. 3.5 explains how our approach satisfies the system requirements. In Sect. 4, we evaluate the implementation of the system. Finally, Sects. 5 and 6 discuss related work and provide conclusions.

2 Use cases and system requirements

In this section, we summarise our use cases for exhibitions, auctions and transport; describe potential attacks; and outline the system requirements.

2.1 Exhibition and auction

In this section, we consider both exhibition and auction scenarios. Figure 1 shows the entities involved and their relations. An entity is represented either as a stylised person or as an object. A line connecting two entities represents some relationship between them.

The following entities are involved: (i) a cultural asset; (ii) the owner of the cultural asset; (iii) a qualified organisation that authenticates the asset, for example, a museum or a research institute; (iv) an official department that manages the qualification of (iii); (v) an exhibitor or a dealer; and (vi) an end user.

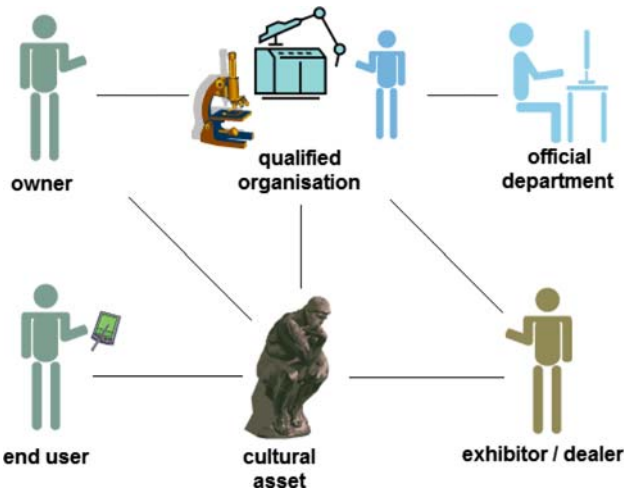

Fig. 1 The entities involved in the use cases

A cultural asset is a valuable object with social or artistic significance. For example, an ancient Roman sculpture or a Picasso painting. The owner can be a person or an organisation. In the exhibition case, the exhibitor hires the cultural asset from the owner; in the auction case, the owner sells the cultural asset through a dealer. In both cases, the cultural asset needs to go through an authentication process. The authentication is performed by a qualified organisation. The qualification is managed by an official department. For instance, in Greece and Italy, the ministries of cultural heritage manage such qualifications. The qualification is granted based on the speciality, the technical strength and the reputation of the organisation. The qualification aims to provide some guarantee of the trustworthiness of authentication results. The same organisation can have different qualifications related to different types of cultural assets that they can authenticate. After authenticating a cultural asset, the organisation generates a certificate vouching for the authenticity of the cultural asset.

If the cultural asset is to be exhibited, then it must be transported to the exhibition site and will remain there until the end of the exhibition. After the exhibition, the cultural asset must be returned to the owner. If the cultural asset is to be sold in an auction then it must be kept securely by the organisation. After the auction, if someone buys it, it must be securely transferred to the buyer; if the auction fails, it must be returned to its owner. The reason why the cultural asset is kept securely by the organisation during the auction is that otherwise the owner and dealer could collude and send a counterfeited asset to the auction and keep the original one.

Of the entities involved, (iii) and (iv) are normally trusted. The organisation that provides authentication of cultural assets is unlikely to cheat because this would damage its reputation and it can be held liable if it is found to be providing false results. The official department has the ultimate responsibility of protecting the authenticity of the cultural assets and should be the most motivated entity to fight the counterfeit of cultural assets. The owner and the exhibitor/dealer are not trusted because they can benefit from counterfeiting the assets. The cultural asset itself is a passive object in the system. The end user is normally the victim of counterfeit cultural assets and in need of protection.

2.1.1 *Potential attacks on exhibitions and auctions*

In the scenarios described above, we highlight the following attacks to the traditional certification system:

- Certificate forgery. An adversary can forge a cultural asset and a certificate from an authority which claims it is an unrevealed work of a famous artist or a newly discovered antiquity.
- Certificate modification. An adversary can modify a certificate to claim it has a higher value.
- Swapping. An adversary who has a cultural asset and its certificate, counterfeits the asset and swaps the real one with the fake one.
- Certificate reuse. An adversary who has a certificate for a cultural asset issued by an authority counterfeits the asset and reuses the certificate.
- Certificate duplication. An adversary duplicates a certificate for a cultural asset issued by an authority, counterfeits the asset and uses the duplicated certificate.
- Certificate replication. An adversary who has the cultural asset obtains different valid certificates and uses them in counterfeit ones.

2.1.2 *Exhibition and auction system requirements*

The goal of our position and time authentication system is to prevent the illegal profits made from counterfeit cultural assets. We describe the use of digital tags to prevent counterfeit cultural assets entering circulation through auctions and detect them from being shown in exhibitions. The high-level requirements of the digital tags are:

- Providing authentication. End users must be convinced they are viewing or buying an authentic cultural asset after they verify its tag.
- Non-forgeable. No one can forge a tag and claim it was generated by a trusted entity.
- Integrity. After being generated, no one can modify the contents of the tag.
- Non-reusable. The tag can be used only once.
- Anti-duplication. It should be hard to duplicate the tag or use the duplicated tags without being detected.
- Tag uniqueness. For each cultural asset there must be exactly one valid tag at the same time.
- Off-line operation. Most of the operations should be able to be performed off-line without recourse to online services.

We emphasise that conventional digital certificates/credentials are non-forgeable and can provide integrity, but they can be easily duplicated and reused. Therefore, as shown in the following sections, our digital tags use position and time information to address the aforementioned problems.

2.2 The transport use case

In Fig. 2 we show all entities involved in the transport scenario, i.e. the owner of the cultural asset, the exhibitor/dealer, the transport company and third-party entities. A transport company transports cultural assets from one place to another. Third-party entities include authorities vouching for the transport content (e.g. insurance companies), experts checking the cultural asset conditions (e.g. the certified organisation), an escort (E) for the transportation (e.g. a security agency or the owner itself) and a monitoring console receiving data during the transport, either the owner or trusted organisations can access it.

Although transportation can be summarised as the act of moving cultural assets between the owner and an exhibitor/seller, in practice it involves complex planning, packaging, journey and delivery phases.

In the planning phase the owner, the exhibitor/seller and third-party entities cooperate to produce several

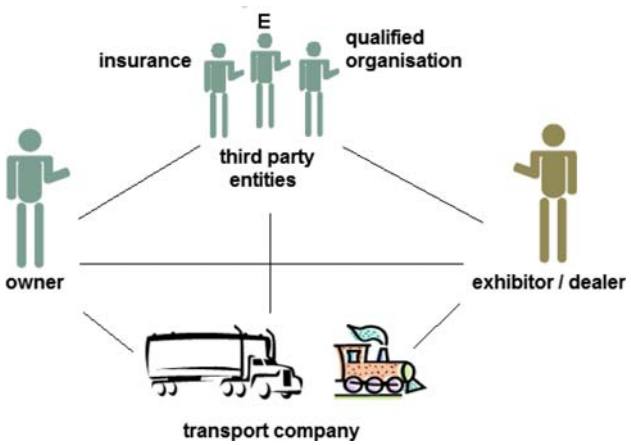

Fig. 2 The entities involved in the transport scenario

documents. For instance, there can be documents describing the set of cultural assets, their conditions, their value in case of damages, the time, start and end points of the journey plus possible paths. In the packaging phase experts package the works of art with special boxes and load the lorry. In the journey phase the assets are monitored in order to be safely delivered to the exhibitor or seller.

Among the entities involved, the owner and the third party entities can be trusted. The owner is normally the victim of thefts. Third party entities are usually entities trusted by the owner and include organisations that are not interested in stealing the assets (e.g. insurance companies) or may have the asset protection as a primary concern (i.e. security agencies and qualified organisations). The exhibitors and dealers cannot be trusted because they can benefit from stealing the assets. The transport companies cannot be trusted since thefts usually happen when objects are managed by transport operators along the route.

2.2.1 Attacks on the transport scenario

In the scenario described above, we highlight the following attacks to the transport system:

- Cultural asset substitution. An adversary substitutes a cultural asset with a fake one.
- Cultural asset theft. An adversary steals some cultural assets.
- Transport diversion. An adversary misleads the security agencies and diverts the lorry along a wrong path in order to steal the cultural assets.

2.2.2 Transport system requirements

The goal of the context-aware transport system is to address the problem of theft during transport. The high-level requirements of the system can be summarised as follows:

- Anti-theft. Any attempt to steal cultural assets must be detected.
- Non-substitution. Any attempt to substitute a cultural asset with a fake one must be detected.
- Path enforcement. Any attempt to divert the transport from the correct path must be detected.
- System security. The system should be robust enough to prevent attacks by itself.

3 Context-aware security for cultural assets

In this section, we describe how the position and time authentication system can be added to the cultural asset life cycle in order to enhance security. Our approach is composed of the following phases: (i) certification; (ii) identification; (iii) transport; and (iv) authentication.

3.1 Certification phase

In the certification phase organisations that claim to be qualified to check assets, e.g. museums, interact with an official department, e.g. a government authority, in order to obtain a digital qualification. This certification phase is composed of two steps: (i) qualification; and (ii) certificate generation. In the first step the organisation contacts the certification authority, completes some forms and proves its identity. The certification authority conducts a comprehensive evaluation of the technical and non-technical merits of the organisation to establish the extent to which the organisation's ability in authenticating cultural assets meets its requirements. If the organisation qualifies, the certification authority generates a certificate for it. The certificate (see Fig. 3) is an X509 v3 digital certificate [10]. This certificate is identified by a serial number and contains: the issuer (e.g. the certification authority) information, the subject (e.g. the organisation) information, the period of validity, the public key of the organisation and the issuer signature. Moreover, the extensions field can contain additional accreditation constraints, for example, the organisation is approved to authenticate certain types of cultural assets. The related private key must be kept safely.[1] For instance in the CUSPIS project the certification authorities are the Italian and Greek Ministries of Cultural Heritage. Certificates have been released to Roman museums and to the National Museum of Athens.

3.2 Identification phase

The identification phase is performed to assign a digital tag to an asset (as we show in Fig. 4). In this phase, a qualified organisation checks the cultural asset. If it is "authentic", the organisation generates a geo-data based tag (GD) for it. A GD (see Fig. 4) contains the following fields: (i) a Unique Code (UC); (ii) the organisation certificate (C); (iii) the destination area (DA); (iv) the start time (ST); (v) the end time (ET); (vi) extensions; and (vii) the organisation signature (S).

The UC field is an identifier that uniquely identifies the cultural asset. The field C contains the digital certificate of the organisation which is generated in the certification phase (see Sect. 3.1). The DA field defines the location, where the cultural asset will be exhibited/sold. The start

[1] In the CUSPIS project, the private keys are generated by the certification authorities and sealed into a tamper-proof device which is delivered securely to the organisations.

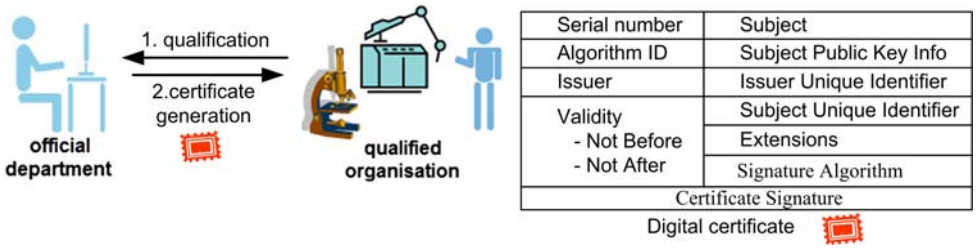

Fig. 3 The certification phase

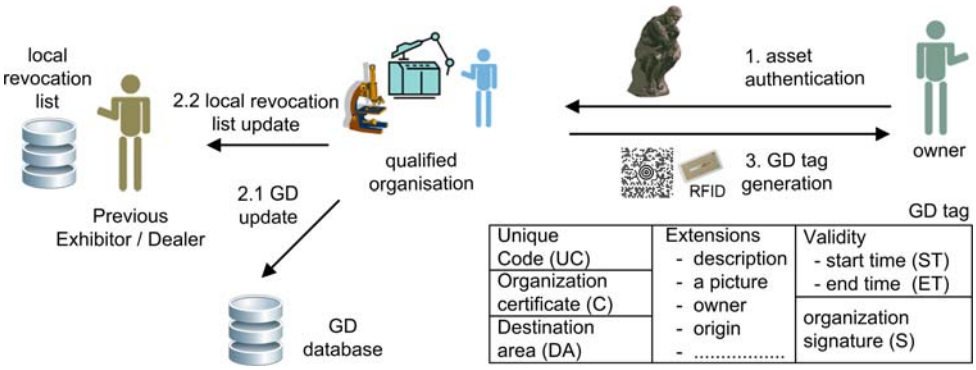

Fig. 4 The identification phase

and end times denote the period in which the cultural asset will be exhibited or the period of the auction. The extension fields contain information for users to uniquely identify the cultural asset, e.g. a description, a picture of the asset and place, the owner, the cultural asset origin and so on. The organisation signature (S) is a standard digital signature of the GD that is generated using the organisation's private key.

The GD can be stored and attached to the cultural asset in different ways. For instance, we use both RFID tags[2] and graphical bar code (e.g. a shot code and QR code) tags to store the GD. The end user can read the RFID tags with a PDA or take a picture of the graphical bar code with a mobile device in order to obtain the GD.

A related problem with tag generation is tag revocation, if for example, an owner wishes to withdraw its cultural asset from an exhibition/auction. To do so the owner shows the GD to the organisation. The organisation verifies the signature S and checks the owner identity. If the GD is successfully verified then the organisation revokes the GD and updates the revocation list. In our implementation revocation lists are updated through a trusted replicated service.

Organisations must take further measures to avoid a replication attack. Replication means there are multiple valid GDs for different purposes or for different places with respect to the same cultural asset. Multiple valid GDs allow the owner to counterfeit the cultural asset and profit from it. For instance an owner can make illegal profits by renting his cultural asset to two different exhibitions. To avoid being detected, he requests a GD for one exhibition. After he obtains the GD, he sends the same item to the organisation and asks another GD for another exhibition. Now that he has two valid GDs, he can counterfeit his cultural asset, send the real one with a valid GD to one exhibition and send the counterfeit one with another valid GD to the other exhibition. Since the end users can only tell whether the cultural asset is authentic by verifying the GD and both GDs are valid, the counterfeit cultural asset will not be detected. To prevent the replication attack, our approach requires a replicated database of GDs shared by all certified organisations. After an organisation authenticates a cultural asset it must query the database with asset information. Currently, cultural asset search is performed based on the cultural asset type, period, weight and author. However, other techniques such as fingerprinting [12] could be used to produce a unique ID for each cultural asset. In the case that a GD is issued and is still valid, the organisation will require the owner to revoke the old one otherwise no new GD will be issued. The database will be updated whenever a GD is generated or revoked.

Although cultural asset authentication requires organisations to use some "complex" components, update a replicated database and have specialised skills [6, 7, 8, 12], users can easily read all GDs and perform offline authentication with simple widespread devices (e.g. a PDA).

3.3 The transport phase

After the identification phase, cultural assets need to be moved to the site of the exhibitor/dealer (in the following

[2] We used RFID tags with 128 KB of memory that maintain full compatibility with the EPC standard [11].

referred to as the renter). To this end we provide a secure transport composed of the following four main steps: (i) planning; (ii) packaging; (iii) the journey; and (iv) delivery.

3.3.1 The planning and the packaging steps

In the planning step different entities cooperate to produce different digital certificates. They must include an authorisation certificate for each package, an insurance certificate and a transportation one.

Each authorisation certificate is produced by the owner and the renter and includes the works of art to be inserted in the same package. The insurance certificate is produced by the owner, the renter and an insurance company and describes the artwork conditions—this allows the owner to claim compensation in case of damage. The same parties along with a transport company cooperate to produce the transport certificate. This defines a secure route, a path where network connections should always be available, and the means of transport used. A route is defined in terms of a list of tuples $\{(A_s,T_{A\_s}), (A_1,T_{A\_1}) \ldots (A_i,T_{A\_i}) \ldots (A_n,T_{A\_n}) (A_d,T_{A\_d})\}$, where A_s is the transport starting area and T_{A_s} the transport starting date (i.e. day, hour and minute), A_i is an area the transport has to pass and T_{A_i} the date it must be passed; (A_d, T_{A_d}) is the destination area and its date.

After the planning step, trusted packaging experts organise the lorry with the right content (see Fig. 5 for a configuration example). They put inside each package: (i) the set of cultural assets defined in the authorisation certificate; (ii) sensors for reading temperature, light and humidity; (iii) motion sensors for detecting movements inside the package; (iv) sensors of distance to measure the distance between two surfaces inside the package; (v) an Asset on Board Unit (ABU) (e.g. a PDA device), where the authorisation, the transport certificate and the protocol implementation are loaded and all sensors are connected. Moreover, a Transport Control Unit (TCU) is installed on the roof of the lorry to forward into the lorry the position and time information provided by the positioning system, for example by the satellite signal.

3.3.2 The journey and delivery steps

The transport protocol used to move cultural assets from the owner to the renter is given in Fig. 6. It uses the following notation and assumptions.

The symbol K denotes a symmetric encryption key and $\{M\}_K$ the message M encrypted with the key K. PK_e and SK_e denote the secret and the public key of an entity e, respectively. For the sake of simplicity the interactions with the positioning system is not shown in Fig. 6—we assume all entities can locally receive broadcasted position

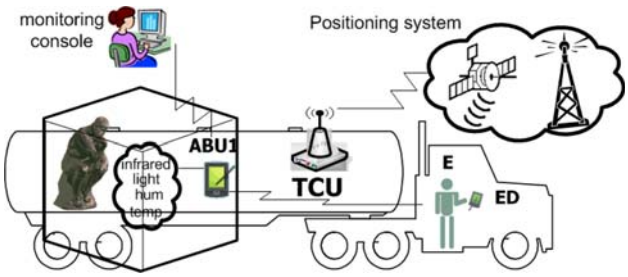

Fig. 5 A transport configuration

and time information. The confidentiality, the integrity and the authentication of this information depends on the positioning system used. For instance the current satellite system (GPS) does not provide these services, while a UMTS-based positioning system can do so.

The journey step begins when the escort (E) gets on the lorry and uses its PDA device (in the following referred to as *ED*) to begin the transport protocol activity. This includes a *startUp* message sent by the ED to each ABU and a set of activities performed by each ABU to validate the *startUp* provided data. The *startUp* message is of the form $\{pos_{ED}, t_{ED}, cred_E\}_{K\_ED,ABU}$, where $cred_E$ are the E credentials, pos_{ED} the ED position, t_{ED} the current time and $K_{ED,ABU}$ a symmetric key shared among the ED and all ABUs. When an ABU receives the message it verifies the E credentials and sends a *posReq* message to the TCU device to obtain the current time–location information. The *posReq* message is of the form $\{ABU\}_{K\_ABU,TCU}$, where ABU is a unique identifier and $K_{ABU,TCU}$ a symmetric key shared between the TCU and all ABUs. The TCU receives the request, gets its current position pos_{TCU} and time t_{ED} from the positioning system and sends the message $TCUPosTime = \{pos_{TCU}, t_{TCU}\}_{K\_ED,ABU}$ back to the ABU. The *ABU* uses both TCU and ED location–time information to perform *checkStartingArea*(). This ensures that the TCU position pos_{TCU} (i.e. the position of the lorry) and ED position pos_{ED} are inside the planned starting area A_d and that the TCU time t_{TCU} and the *ED* time t_{ED} coincide with t_d. We emphasise that when an *ABU* fails to contact the *TCU*, it sends an alarm to both *ED* and monitoring console. A *TCU–ABU* communication failure can be a consequence of a package theft or a *TCU* failure.

In the aforementioned starting activity, the use of time and location ensures where the lorry is starting and when the entities planned. The symmetric key $K_{ED,ABU}$ ensures confidentiality and escort authentication.

If all checks are successfully performed each ABU can start performing its main activities, i.e. sensor reading, report sending and area coverage check.

The sensor readings are used to detect attempts of package unwrapping and are performed by invoking the

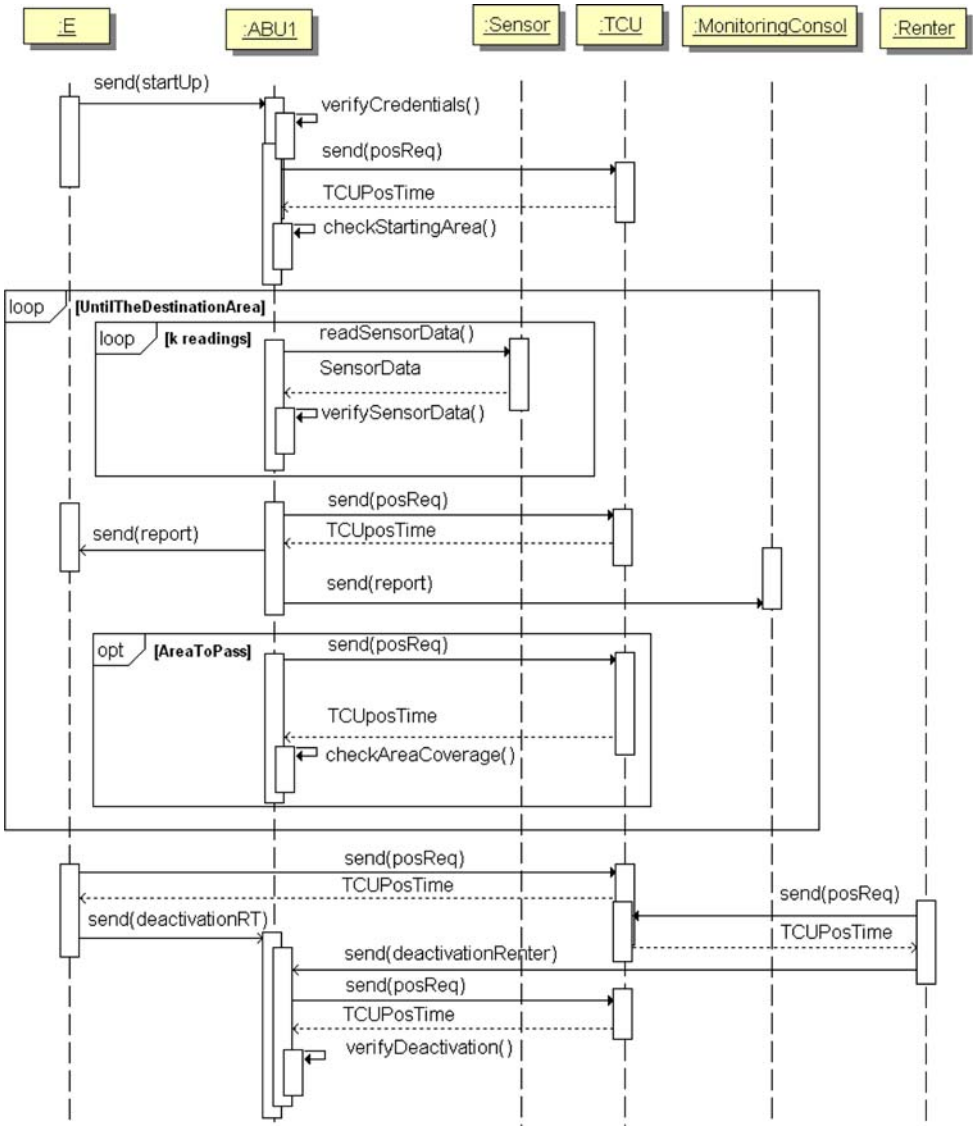

Fig. 6 The transport protocol

procedures *readSensorData* and *verifySensorData* (see the inner loop of the sequence diagram of Fig. 6). The *readSensorData* call is performed through a secure channel and is used to acquire all sensor readings, i.e. temperature, light, humidity, distances and movement readings. The *verifySensorData* procedure reads each data (e.g. the light L), fetches the data of the same type acquired in the previous reading activity (e.g. L_{pre}) and evaluate the difference $|L-L_{pre}|$. When this difference exceeds a threshold (e.g. Δ_L for the light) an alarm is sent to both the ED device and the monitoring console. The reliability of package unwrapping detection depends on: (i) ensuring that there are different values of temperature, humidity and light between the environment inside and outside the packages and (ii) ensuring that the thresholds are correctly set.

Differences between the inside and outside sensor readings are vital in detecting unwrapping. When the differences are significant, any attempt to unwrap the package will cause variations in sensor readings big enough to trigger alarms. Differences in sensor readings can be achieved by having packages with their own internal conditions that are isolated, as much as possible, from the external ones. For instance light and humidity can be isolated with packages composed of isolating materials (e.g. polystyrene and silicone). Humidity differences are a consequence of the material by being transported (e.g. wood, terracotta or ceramic) and can be modified using dehumidification materials. For temperature, a small heater can be connected to a thermostat for constant values.

A correct threshold setup is needed to tolerate the differences between two consecutive readings in order to maximise the unwrapping detection and minimise false alarms. In cases of distance, movement and light readings

the threshold can be set almost to zero[3] since each package is closed and its internal structure does not change. A slightly higher threshold can be set up for temperature and humidity since they may be subject to slightly bigger variations during transport and weather conditions. Despite the aforementioned measures, false alarms are still possible, e.g. when there is an unexpected change in environmental conditions. Our system has been implemented to support false alarm detection. In particular, a false alarm is triggered by the system when different alarms are observed, at the same time, in different packages. This is based on the assumption that all packages should be equally affected by changes in context and incorrect threshold setup. This false alarm detection is performed in both the ED and the monitoring console.

An adversary trying to subvert the aforementioned measures must breach different security defences implemented by different sensors. Sensors for distance and motion detection are pointed inside the package onto different surfaces, therefore any unwrapping can be detected. Even if, the adversary breaches this first line of defences and penetrates an area where no sensor is pointing, he must create an external environment equal to that of the package. Also, the trusted parties (i.e. the packaging experts, owner and escort) can hardly approximate the internal package conditions knowing the starting ones (e.g. heater, insulating /dehumidification materials).

After k sensor reading activities each ABU builds a *report* message $\{pos_{TCU}, t_{TCU}, Info\}$, where pos_{TCU} is the current position, t_{TCU} the current time, and *Info* some ABU information—the ABU state and its identifier. This is encrypted with the key $K_{ED,ABU}$ and is sent to the ED. The purpose of this message is twofold: first it provides some information about the device. Second it is used by the ED to detect ABU faults and package thefts which cause loss of signal with the ED. The time–location information plays an important role in the security of the protocol itself since it is a fresh nonce to avoid replay of old reports, i.e. an adversary that keeps sending an old report, while stealing the package. The same report is encrypted with a key $K_{ABU,MC}$ shared between all ABUs and the console, and sent to the monitoring console. The monitoring console uses the signal to verify the presence of the ABU with a less restrictive availability constraint. In fact, despite good route planning, devices can stop sending data because of a tunnel or changes in the mode of transport.

During the journey, the ABUs also read the current time t and the position P from the TCU and check whether t is the time at which an area A_i must be passed. If this is the case the ABUs perform an area coverage check by invoking the procedure *checkAreaCoverage*() to verify that the position P is inside the area A_i. If the check verifies that at each planned time the lorry is in the planned area, we are assured that the transport follows the right path. It is worth mentioning that each area should be chosen to be big enough to avoid false alarms. In fact delays can affect the time at which the area A_i is going to be reached.

The delivery step is performed when the lorry is in the destination area. In this step the E and the renter send a deactivation message to all ABUs. The former is a message $deactivationE = \{cred_E, pos_{ED}, t_{ED}\}_{K\_ED,ABU}$, where $cred_E$ are the E credentials, pos_{ED} the current ED position, t_{ED} the current time and $K_{ED,ABU}$ is a symmetric key shared between the ED and all ABUs. The latter is a message $deactivationRenter = \{cred_{Renter}, pos_{Renter}, t_{Renter}\}_{K\_Renter,-ABU}$, where $cred_{Renter}$ are the renter credential, pos_{Renter} the renter location, t_{Renter} is the current time and $K_{Renter,ABU}$ is a symmetric key shared between the renter and all ABUs. Each ABU receives the requests, verifies the credentials, checks that the TCU, the renter and the ED positions are in the destination area and verifies that the TCU, the ED and the renter time match the destination time. When all checks are successfully performed each ABU deactivates the monitoring activities, generates a deactivation receipt and sends it to the monitoring console.

3.4 The authentication phase

In the authentication phase (see Fig. 7), the end user reads a GD and verifies the authenticity of the related cultural asset. To this end the user employs a mobile device (e.g. a PDA) equipped with a verification component, a history list, two revocation lists and a time component. The main steps performed in the verification process are *revocation checking, digital certificate verification, GD digital signature verification, position and time verification, object verification* and *duplication checking*.

In the *revocation checking* step, the verification component verifies that the GD is not present in the GD revocation list.[4] The GD revocation list can be downloaded from a trusted web site and installed prior to the verification. In particular, if a user has decided the places he wishes to visit (cities/museums/auctions), only the revocation lists for those places need to be downloaded.

In the *digital certificate verification* step the verification component reads the certificate (C) contained in the GD tag and performs the usual verification on digital certificates [10]. The public key of the certification authority and revocation lists can be downloaded from a trusted web site and installed prior to the verification.

[3] Small fluctuations may be consequence of hardware imprecision.

[4] The search inside the revocation lists is performed based on the GD digital signature S, the UC code and the owner.

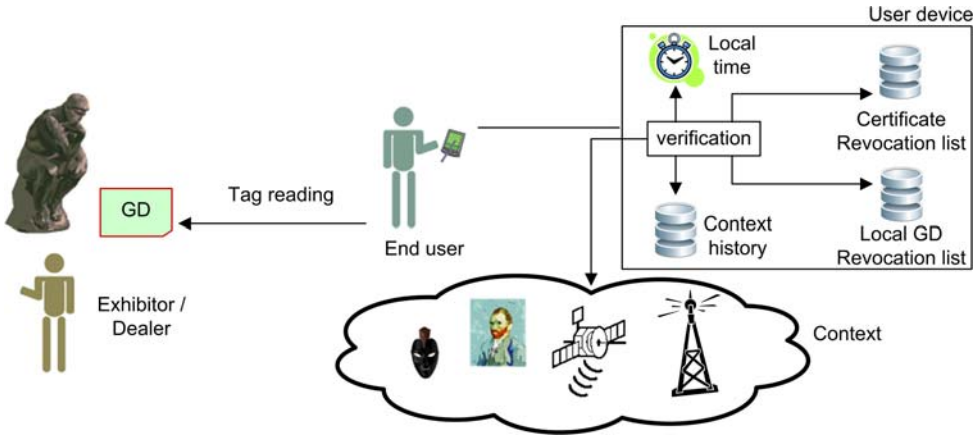

Fig. 7 The authentication phase

In the *GD digital signature verification* step, the verification component reads the signature field (S) from the GD and verifies it by using the public key retrieved from the certificate (C).

In the *position and time verification* step, the verification component contacts the positioning and the time component to get the user's current position and time. It is worth noting that the positioning and the time component must ensure the correctness of the information they provide, this can be done by signal authentication and cross-checking. For instance, the Authentication Navigation Messages (ANM) service [13] for the upcoming Galileo satellite system could be used for providing reliable position information. The verification component verifies that the current user position is inside the destination area (DA) contained in the GD tag. Moreover, it verifies that the current time is greater than the start time (ST) and less than the end time (ET).

In the *object verification* step, the verification component verifies that the characteristics of the cultural asset and place meet the identification information contained in the extension field of the GD. The end user is involved in this step. The verification component presents the identification information to the end user and the end user provides the verification result.

If any of the steps fail, then the authentication fails. Otherwise, the verification component checks the authentication history in the period of this exhibition tour/auction to see whether the GD has been duplicated, i.e. performs a *duplication checking* step.

In the exhibition case, the authentication history is a sequence of (*GD*,*POS*) tuples, where *GD* is a verified tag and *POS* is the user position when this tag was read. Suppose that a user is verifying a tag *GD* at the position *POS*, and a tuple (*GD*,*POS*′) is in the authentication history (i.e. the tag GD has already been visited). Then, when *POS* is sufficiently far from *POS*′ the verification component concludes that the tag has been duplicated. As discussed in Sect. 4 the notion of sufficiently far is strictly related to the technologies used to implement the system.

In the auction case, the authentication history is just a sequence of verified GDs, this is because in the auction, the cultural assets are presented one after another and the user does not change the position. If any GD in the sequence is the same as the one being verified, a duplication is detected. When the verification component detects a duplication, it raises an alarm and marks both as duplicated.

If all the steps succeed, then the authentication succeeds and the end user can be assured that the cultural asset is not counterfeited.

3.5 Remarks

This section explains how our approach satisfies the requirements in Sect. 2.

The first major requirement of our system is to provide a mechanism for authenticating cultural assets to end users. Cultural asset authentication is not easy because it requires dedicated equipment and skills. End users usually do not possess such equipment and skills. In order to solve this problem, an object which is easy to authenticate by end users is created by a trusted organisation for an authenticated cultural asset and is bound to the asset. The authentication of a cultural asset is then realised by authenticating the object bound to it. The main concerns in this approach are: first, the binding can be broken (for example, a certificate can be attached to a counterfeit asset), second, adversaries can make considerable profits by breaking the binding, therefore they are highly motivated to do so, third, the objects itself need to be non-forgeable and tamper-proof.

Our solution uses GD, a digital tag, to address the aforementioned problems. The binding between GDs and authenticated cultural assets are strengthened by position and time information, digital certificates, a centralised DB,

revocation lists and identification information stored in GDs. Position and time information is also used to achieve the goal that even if a binding is broken, it is hard to take any advantage from it. Digital signatures make it impossible to forge or modify GDs. Regarding the attacks listed in Sect. 2.1, forgery and modification attacks are hard because an adversary must break our underlying crypto-systems first. The crypto-system has been formally described and security properties formally verified in [1]. The swapping attack is not possible in the auction case because the asset is kept by a trusted organisation which authenticates the asset and delivers it directly to the buyer or the owner after the auction. The swapping attack is possible in the exhibition case but the exhibitor has paid for the loan of the cultural asset and has permission to exhibit it in the exhibition, so there is no reason for the exhibitor to exhibit a counterfeit item, while holding the real one. Reuse and duplication attacks can be detected because GDs are only valid in a specific position and at a specific time. Under such constraints, any reuse or duplication of GDs outside the time period or the location area will simply make the GDs invalid. Reused or duplicated GDs with the correct position and time will not give any advantage to an adversary and will be detected by checking the authentication history. Replication attacks can be prevented by revocation lists and the centralised DB as discussed in Sect. 3.2.

The second major requirement of our system is to provide a secure transport for cultural assets. Our system uses position, time and sensor readings to enforce the requirements of physical security. As discussed in Sect. 3.3, any attempt to steal, to substitute the cultural assets or to divert the transportation route will be detected. We also designed a cryptographic protocol to ensure the integrity and confidentiality of the data communication. Data is accepted only if it comes from a trusted source and is fresh, therefore an adversary cannot manipulate the data in order to mislead the system. Sensitive data is encrypted, so an adversary cannot get useful information by eavesdropping.

4 Implementation

Our system was implemented and tested in the context of the CUSPIS project [14] and is being used as a commercial product for transport and asset authentication [15].

4.1 Cultural asset authentication

Our system was used for both an outdoor and several indoor exhibitions, where government and qualified parties were involved.

4.1.1 Outdoor exhibition

The outdoor exhibition was organised in Hadrian's Villa near Tivoli (Rome). This villa was built by Emperor Hadrian as an Imperial palace and is the most extensive ancient Roman villa, covering an area of more than 80 ha. In this scenario the Italian Ministry of Cultural Heritage took the role of the official department and the National Museum of Rome was the qualified organisation. The positioning system used was the European Geostationary Navigation Overlay Service (EGNOS), a precursor of the Galileo satellite [16].

Each cultural asset was equipped with an RFID device, where the related GD is written. The destination area was represented as a polygon (i.e. an ordered list of points), where each point is a pair of values representing longitude and latitude. For instance the area {(41.94231,12.77278), (41.94222,12.77538), (41.94139,12.77529), (41.94142,12.77267)} identifies the position of a Roman sculpture inside Villa Adriana. Each user had a PDA device equipped with both an RFID reader and a GPS receiver. The device reads the RFID information, a local key store, the satellite time–positioning information, the authentication history and automatically checks the cultural assets authenticity. History authentication was used to check duplication as described in Sect. 3.4 by taking into account the range of our RFID tags. If the user's PDA reads the same tag GD in two different positions POS and POS' then, when they differ by more than the RFID radius range a duplication is found. It is worth noting that within the RFID radius range the same GD will be quickly detected.

In Fig. 8 we show part of Hadrian's Villa where, the aforementioned sculpture is located. The RFID of the sculpture is physically bound to its base. On the left side of the picture we show the graphical user interface, where the map of the villa is shown. This map highlights all cultural

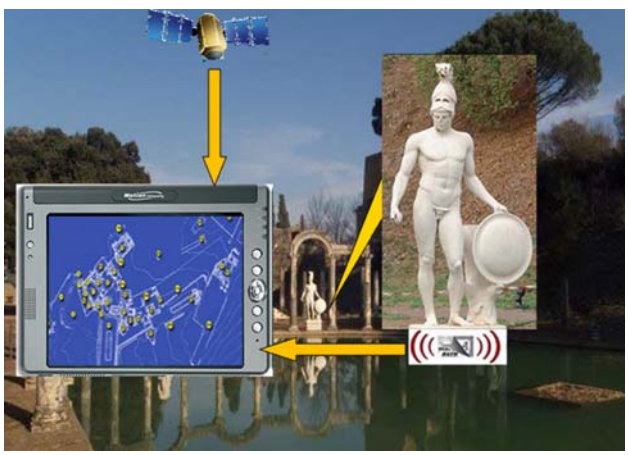

Fig. 8 A Roman sculpture exhibited in Villa Adriana

asset locations and the current user position. It is worth noting that if the sculpture had been non-authentic a warning message would have been shown on the mobile device.

4.1.2 *Indoor exhibitions*

The indoor exhibitions were organised in the National Museum of Athens and in several sites located in Rome. In this case the Italian and Greek ministries of cultural heritage took the role of official departments. Qualified organisations were the National Museum of Athens and Roman museums.

In some exhibitions, GDs were written in a RFID located next to the cultural assets. The position and time information were encoded as a mail address (Roman temporary exhibition, via Dante Alighieri, n 34B, floor 2) and a period (i.e. from 1 Sep 2008 until 10 Sep 2008), respectively. All users could receive both cultural asset information and position–time information on their devices. While GD integrity, and the authenticator's authenticity were automatically verified by the user device, the users had to read and validate the position–time information. In this case the history was built using an indoor positioning system (it was used also to provide cultural asset information) in order to relate to each *GD* the user position. A similar indoor exhibition case study was performed in Rome writing each GD onto a graphical code located next to its cultural asset. The destination area was identified using the UMTS antenna code. Users were equipped with a cell phone and they could take a picture of the code using the encoded information to automatically verify both GD authenticity and position–time data.

In Fig. 9 we show the graphical user interface of the indoor visit. It displays two paintings exhibited in Florence. In this case information was stored in graphical codes located next to the paintings. A camera was used to retrieve the data and a component of the PDA was installed to verify the authenticity of all information. Note that a user can use the images to visually verify that the paintings are the ones to be authenticated.

Several GDs for different cultural assets were loaned to several museums [9]. In each museum mobile devices were used to locally perform the authentication of cultural assets in an efficient and fast manner.

Our system has minimal cost for both organisations and end users. Organisations require a normal PC and our implementation to generate the GD. When GDs are written as graphical bar codes the museum needs only to buy the kit and they can easily print the code onto a piece of paper. When GDs are written to RFIDs the organisation must add the cost of the RFIDs. Users require a cell phone with RFID/GPS capability and a camera when GDs are stored as a graphical bar code.

4.2 The transport case study

We have applied our transport system to move cultural assets from Rome (*Scuderie del Quirinale*) to Tivoli (Hadrian's Villa).

In the planning phase the Ministry of Cultural Heritage, the *Scuderie del Quirinale* (a Roman exhibition site) and the museum of Hadrian's Villa cooperated to decide which assets to move. The same entities cooperated with an insurance company to produce an insurance certificate and with a specialised transport company to produce a transport certificate (see on-line documentation reported in [9] for a detailed description). After this planning phase all ABUs, the TCU and the ED were loaded with, all certificates, our system implementation and with all symmetric keys.

During the packaging phase experts placed each cultural asset into a special box made of wood, polystyrene and silicone. As shown in Fig. 10 each asset was carefully handled and was put inside the box after configuring the related ABU.

After packaging the escort uses his ED (shown in Fig. 11) to signal the start of the journey. During this

Fig. 9 A picture displayed on the indoor visit

Fig. 10 The packaging phase

Fig. 11 The escort's device

Fig. 12 The CUSPIS centralised monitoring console

phase he receives information about the current position and all ABU reports. At the same time, reports are also sent to the monitoring console shown in Fig. 12. There an operator is responsible for checking that no alarm is raised and that the transportation vehicle follows the planned route. In our journey from Rome to Tivoli no false alarm was detected by the sensor reading activities and the escort's device correctly received reports. However, the centralised console received some alarms due to delays on report deliveries. In this case an agreement between the escort and the console operator was sufficient to solve the problem.

In the reception phase all ABUs were correctly deactivated and a receipt of transportation was generated.

5 Related work

In this section, related work for both cultural asset authentication and secure transport is summarised.

Concerning cultural asset authentication, we include systems supporting exhibitions; some because they present approaches to discourage imitations of valuable assets, others because they use position and time information for authentication purposes. We also consider RFID and graphical bar code technologies since they share our counterfeiting and integrity problems.

Systems with auto-localisation functionalities are now available to help people visiting museums avoid traditional audio/visual pre-recorded guides. For instance, MAGA [17] is a user friendly virtual guide, that provides cultural asset information on PDAs. The interaction between the application running on the PDA and the environment is triggered by the detection of both passive and active RFID tags. A passive RFID is used to hold a unique ID for the cultural asset. The ID is passed to the server application via Wi-Fi in order to retrieve cultural asset information. The active RFID holds the cultural asset data directly and allows offline operation without an online server connection. Mobile applications have also been experimented in [18, 19], where mobile devices perform local and remote connections to get cultural asset information. Although the aforementioned systems improve the user experience in museum visits they do not address security concerns. Cultural asset information received on a user's mobile device can be easily copied and used for counterfeit assets.

ETG (Traceability and Guarantee Label) [20] presented recently in Vicenzaoro Winter adds to a traditional bar code, an encrypted one that contains asset information signed with the producer's private key. Although the digital signature provides data integrity it does not protect against a duplication attack since all encrypted data can be reused and copied.

RFID technology shares many of the counterfeiting and integrity problems [21]. Passive RFIDs have been successfully applied to identify, catalogue and track valuable assets [22, 23]. They bring real-time, read–write data tracking and process history, useful for producers and users. However, passive RFIDs containing non-encrypted information are not useful for authentication and integrity purposes. To solve this problem two companies, Texas Instruments and VeriSign Inc., have proposed a 'chain-of-custody' approach [24]. Their model involves managing a PKI infrastructure and signing the RFID information with

private keys in order to provide the integrity service. However, digital signatures do not confer cloning resistance to tags. They prevent forging of data, but not copying of data. A solution to cloning and corruption of passive RFIDs can be offered by active ones [21, 25, 26]. They offer anti-cloning mechanisms and hold private keys to perform authentication and establish encrypted communication. However, advanced RFIDs still allow certain attacks. Although anti-cloning RFIDs cannot be duplicated, they can be reused. And since they can be physically handled by an adversary, they can be breached with appropriate technologies. They also require dedicated devices and exclude other kinds of storage (e.g. graphical bar codes).

Counterfeiting and authentication of assets is so important that international organisations are trying to address it. For instance the EPC global standard for RFID technologies proposes global object naming services [27] that provide each object a unique ID. A centralised database stores asset information that can be used to authenticate and verify the product authenticity. However, this centralised DB poses scalability problems, requires a user to establish a remote connection and require time–space information to avoid duplication of asset information. In our approach organisations coordinate to maintain a replicated database of GDs, and users perform offline GD verification and thus scalability is enhanced.

In [28] intrusion detection techniques are applied to detect cloned data. This approach is prone to false alarms that are not allowed in our system implementation (especially in the case of auctions). The false alarm rate is reduced in the approach presented in [29], where they provide a probabilistic-based approach for location-based authentication. They use past location of products to detect counterfeit assets. However, our system starts from different assumptions, in fact very often previous locations of a cultural asset are unavailable but where it will be exhibited is known a priori. Since we are dealing with highly valuable objects no false alarms are permitted. Moreover, we have introduced different security measures (especially in the same destination area) to ensure security properties.

In [5] location information is used to address the forgery of origin information and the transport problems of assets. Each asset is equipped with a tag that contains origin and tracking information signed with the producer's private key. Tags can be read by users for origin information and a centralised DB is used for asset authentication. In our system we perform offline authentication verifications. We add the concept of time and authentication history to address the problem of duplication in the same area. Moreover, our approach have been formally described and security properties formally verified [1].

Concerning the secure transport of assets we cite systems that try to monitor the correct route of the lorry and others used to prevent thefts of objects during their journey.

Different approaches can be used to ensure that a lorry follows the right path. For instance tachographs are used in heavy vehicles to monitor drivers' hours but as a secondary purpose they can also be used for the detection of fraud [30]. Tachograph charts are often acquired by the police and used to analyse lorry routes to find out whether they are used for drug smuggling, unlicensed toxic waste and black market activities. Since we are dealing with high-value objects this offline investigation is not adequate. In fact any suspicious activity must be prevented in advance and monitored during the journey.

GPS Tracking Units [31] are used to locate and monitor the vehicles continuously. They are covert and can be hidden in any car, truck, motorcycle, trailer, or motor home. Driver-based companies, police and users can install them and use available Internet services to access different online information, e.g. vehicle location history, its speed and direction of travel. While these services can provide quick tracking information they still suffer from coverage issues. In fact the GPS signal can become unavailable or weak because of tunnels, tall buildings and even trees. Furthermore, GPS systems ensure the lorry path but do not prevent unwrapping of packages.

Asset protection is often provided through specialised transport companies [5] that make use of special packages, strongboxes and security escorts. However, as we pointed out, thefts can be a consequence of several operators that handle the packages and substitute the content. In our approach no entity can open the package during the journey. Only when the recipient and the escort are in the right location can the packages be unwrapped. In this way the location and the time become part of the unlocking key.

6 Conclusion and future work

In this article we have described a context-based system for the authentication and secure transport of cultural assets. Cultural asset authentication is provided by combining both position and time information as well as traditional security mechanisms to generate a position and time-based tag for each cultural asset. This tag is then used to detect or prevent various attacks, such as duplication, reuse and modification. The approach effectively prevents the introduction of counterfeit cultural assets and has been validated in several real case studies. The secure transport service uses position, time and sensor information, such as temperature, humidity and light. It ensures that the transportation vehicle follows the right route and that no package can be opened undetected before the right area is reached

and the authorised entities deactivate the system. In this way the keys of entities are not sufficient to open the packages unless the right destination is reached.

As future work we aim to extend and generalise the use of position and time information to authenticate other kinds of assets (e.g. jewels, watches and wines), as well as verify the physical characteristics of locations (e.g. the exhibition room).

Acknowledgments This research was supported by UK EPSRC research grants EP/D076633/1 (UBIVAL) and EP/C537181/1 (CAREGRID). We would also like to thank the members of the Policy Research Group at Imperial College, and the CUSPIS partners: the Next S.p.A. research group, Vodafone, and the Italian and Greek ministries who supported our case studies.

References

1. Mostarda L, Dong C, Dulay N (2008) Place and time authentication of cultural assets. In: 2nd Joint ITRUST and PST conferences on privacy, trust and security (IFIPTM 2008)
2. Center of Study TCI: Dossier of MUSEUM (2006) http://www.touringclub.it/ricerca/pdf/DOSSIER_MUSEI_2007.pdf
3. Artprice: 2006 Art Market Trends, Tendances du marche' de l'art (2006) http://img1.artprice.com/pdf/trends2006.pdf
4. Jacob J (2002) Counterfeit art—how to keep it out of your collection. Chubb Collectors
5. Mostarda L, Tocchio A, Inverardi P, Costantini S (2007) A geo time authentication system. In: Proceeding of IFIPTM 2007
6. Radiocarbon Dating (2002) BBC on line resource. http://www.bbc.co.uk/dna/h2g2/A637418
7. Thermoluminescence (2002) Minnesota State University. http://www.mnsu.edu/emuseum/archaeology/dating/thermoluminescence.html
8. Klarreich E (2004) Con artists: Scanning program can discern true art. science news 166:340
9. CUSPIS demonstration and performance evaluation report (2007) CUSPIS official home page. http://www.cuspis-project.info/demonstrations.htm
10. Stallings W (2006) Cryptography and network security: principles and practice, 4th edn. Prentice Hall
11. Web page on EPC global organization (2008) http://www.epcglobalinc.org/home
12. Buchanan JDR, Cowburn RP, Jausovec AV, Petit D, Seem P, Xiong G, Atkinson D, Fenton K, Allwood DA, Bryan MT (2005) 'Fingerprinting' documents and packaging. Nature 436:475
13. Pozzobon O, Wullems C, Kubic K (2004) Secure tracking using trusted GNSS receivers and Galileo authentication services. J Glob Position Syst 3:200–207
14. Cultural Heritage Space Identification System (CUSPIS) (2007) European Commission 6th framework program—2nd call Galileo joint undertaking. http://www.epcglobalinc.org/home
15. Next SpA company (2008) http://www.next.it/site/Home.aspx?content=trasporti
16. Official web page of Galileo (2008) http://www.galileoju.com
17. Augello A, Santangelo A, Sorce S, Pilato G, Gentile A, Genco A, Gaglio S (2006) Maga: a mobile archaeological guide at Agrigento. University of Palermo, ICAR_CNR
18. Pilato G, Augello A, Santangelo A, Gentile A, Gaglio S (2006) An intelligent multimodal site-guide for the "parco archeologico della valle dei templi" in Agrigento. In: Proceedings of first European workshop on intelligent technologies for cultural heritage exploitation, at the 17th European conference on artificial intelligence
19. Park D, Nam T, Shi C, Golub G, Loan CV (2006) Designing an immersive tour experience system for cultural tour sites. In: Chi '06 extended abstracts on human factors in computing systems edition, April 22–27. ACM Press, Montréal, Québec, Canada, pp 1193–1198
20. Vicenzaoro winter: Traceability and guarantee label (2007) http://www.vicenzafiera.it/uk/rassegna/vioro1_2007/crapanzano_en.doc
21. Juels A (2006) Rfid security and privacy: a research survey. IEEE J Sel Areas Commun
22. Caputo T (2005) Rfid technology beyond wal-mart. WinesandVines
23. Web page of the TagStream Company (2008) http://www.tagstreaminc.com
24. Texas Instruments and VeriSign, Inc. (2007) Securing the pharmaceutical supply chain with RFID and public-key infrastructure technologies
25. Juels A, Weis SA (2005) Authenticating pervasive devices with human protocols. In: Shoup V (ed) CRYPTO. Volume 3621 of lecture notes in computer science. Springer, pp 293–308
26. Tuyls P, Batina L (2006) Rfid-tags for anti-counterfeiting. In: Pointcheval D (ed) CT-RSA. Volume 3860 of lecture notes in computer science. Springer, pp 115–131
27. EPC global standard powered by GS1: Object Naming Service (ONS) 5 Version 1.0 (2005)
28. Mirowski L (2006) Detecting clone radio frequency identifications tags. Bachelor's Thesis, School of Computing, University of Tasmania
29. Lehtonen M, Michahelles F, Fleisch E (2007) Probabilistic approach for location-based authentication. In: 1st International workshop on security for spontaneous interaction IWSSI 2007
30. Anderson RJ (1998) On the security of digital tachographs. In: ESORICS '98: proceedings of the 5th European symposium on research in computer security. Springer-Verlag, London, UK, pp 111–125
31. A GPS based monitoring system (2008) http://www.vehiclegpstrackingsystem.com/