Place and Time Authentication of Cultural Assets

Leonardo Mostarda, Changyu Dong, and Naranker Dulay

Abstract This paper proposes a place and time authentication system for cultural assets. We develop a protocol that combines traditional cryptographic techniques with place and time information to generate a *secure* tag for each cultural asset. We model the attacker capabilities and show that our secure tag helps ensure the authenticity of works of art. Our system has been deployed and validated in Italian and Greek museums in the context of CUSPIS project.

1 Introduction

Art appreciation dates back more than two-thousand years when Roman sculptors produced copies of Greek sculptures for religious inspiration or simply for aesthetic enjoyment. Over the years art has become a commercial commodity and unauthorised copying an illegal but highly profitable business. Counterfeit cultural assets are sold in auctions and even exhibited around the world. The trade in counterfeit artworks and antiques is a six billion dollar per year business and the largest crime after drug and gun trafficking [1]. For instance in Operation "Canale", the Italian police sequestered 20,000 pieces of paintings and graphics works. Of all the pieces, 17,000 of them were imitations and ready to be sold. In 2006 about 2,000 Italian and French exhibitions were visited by 44 million people with an average fee of 6.3

Leonardo Mostarda
Department of Computing, Imperial College London, London, UK SW7 2AZ e-mail: lmostard@doc.ic.ac.uk

Changyu Dong
Department of Computing, Imperial College London, London, UK SW7 2AZ e-mail: cd04@doc.ic.ac.uk

Naranker Dulay
Department of Computing, Imperial College London, London, UK SW7 2AZ e-mail: nd@doc.ic.ac.uk

euros per person [2]. It has been estimated that five percent of such profits have been made by exhibitions of counterfeit cultural assets.

The main reason for the increase in criminal activity is the inadequacy of countermeasures. Traditionally, the authenticity of a cultural asset is provided by a paper certificate issued by a recognised authority such as a museum. The experts from the authority examine the provenance, i.e. the documented history of the asset, the style of the artist, and they use forensic methods (e.g. carbon dating [3], thermoluminescence [4] and statistical analysis of digital images [5]) to verify the authenticity of the cultural asset. If they believe this asset is authentic, they sign a certificate containing details of the cultural asset.

The main problem with paper certificates is obvious: the certificates can be forged or duplicated and then presented with counterfeit works of art that are shown in an exhibition or sold in an auction.

This paper describes a novel place and time authentication system to detect counterfeit cultural assets. The system generates a tag for each cultural asset that holds the location where, and the time when, the cultural asset can be shown, as well as a cultural asset description, for example, a picture or text signed by an authenticator. Visitors to an exhibition, or potential buyers at an auction can read the cultural asset's tag and use location and time data to check the authenticity of the asset. The digital signature is used to ensure the integrity of the tag data and the authenticator's identity. Although a valid tag can still be copied by an attacker, its use in a different place and time is detectable. To mitigate the tag duplication and reuse problem in the same place and time, the authentication process provides a history-based check and also signed descriptive information for users to check. The history based check analyses each new tag to determine if it is a previously verified tag or if it is a duplicated tag, while the descriptive information can include photos of the asset and place in the tag.

In this paper we formalise the place and time authentication system and establish a threat model. We then show that the system ensures the authenticity of cultural assets. The system has been validated in the context of the CUSPIS European project [6]. For outdoor use, it uses EGNOS, the European Geostationary Navigation Overlay Service, a precursor of the Galileo satellite infrastructure[7]. For indoor use it requires users to check location information stored in RFID and graphical bar codes that users download and run on their mobile device (e.g. PDA or smart phone). It should be pointed out that the approach is independent of the location service, for example, we could use cell-tower or wifi access-point triangulation for indoor applications.

The paper is organized as follows. In Section 2, we describe the use cases, the threat model and the system requirements. In Section 3, we provide an overview of the place and time authentication system. In Section 4, we define the formal model of our system and provide security proofs. In Section 5, we evaluate the implementation of the system. Finally, sections 6 and 7 discuss related work and provide conclusions.

2 Use cases and system requirements

In this section, we motivate our approach with two use cases, highlight potential attacks and outline the overall requirements of the system.

2.1 Use cases

We consider two different but similar scenarios, namely exhibitions and auctions. Figure 1 shows the entities involved and their relations. An entity is represented either as a stylized person or as an object. A line connecting two entities models some relationship between them.

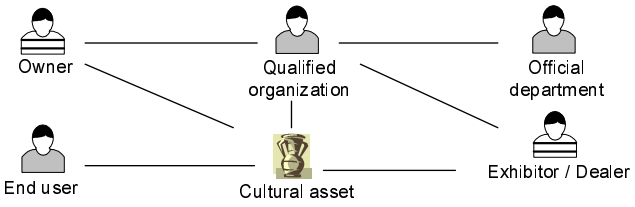

Fig. 1 The entities involved in the use cases

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

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 e..g museum. 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 of such organisations 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 on 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 certification 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 remains 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.

Among all the entities involved, (iii) and (iv) can usually be trusted. The organisation that provides authentication of cultural assets is unlikely to cheat because this will damage its reputation and it can be held liable if found providing false results. The official department has the ultimate responsibility of protecting the authenticity of the cultural assets and is the one motivated most to fight counterfeit 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.

2.2 Threats and potential attacks

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

- Certificate forgery. The attacker 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. The attacker can modify a certificate to claim it has a higher value.
- Swapping. The attacker who has a cultural asset and its certificate, counterfeits the asset and swaps the real one with the fake one.
- Certificate reuse. The attacker who has a certificate for a cultural asset issued by an authority counterfeits the asset and reuses the certificate.
- Certificate duplication. The attacker duplicates a certificate for a cultural asset issued by an authority, counterfeits the asset and uses the duplicated certificate.
- Certificate replication. The attacker who has the cultural asset obtains different valid certificates and uses them in counterfeit ones.

2.3 System requirements

The goal of our place and time authentication system is to stop the illegal profits made from counterfeit cultural assets. We propose 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 place and time information to address the aforementioned problems.

3 Overview of approach

In this section we show how our place 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) tag generation and revocation; and (iii) authentication.

3.1 Certification phase

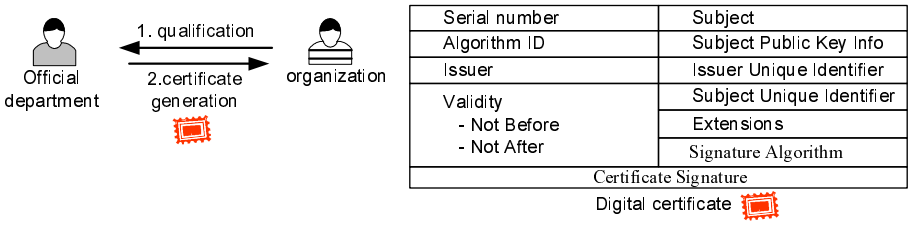

Fig. 2 The certification phase

In the certification phase organisations that claim to be qualified to check assets (e.g. a museum) interact with an official department (i.e., a government authority) in order to obtain a digital qualification. This certification phase is composed of two

basic steps: (i) qualification; and (ii) certificate generation. In the first step the organisation gets in touch with the certification authority, fills on some forms and proves its identity. The certification authority conducts a comprehensive evaluation of the technical and nontechnical merits of the organisation to establish the extent to which the organisation's ability in authenticating cultural assets meets its set of specified requirements. If the organisation qualifies, the certification authority generates a certificate for it. The certificate (see Figure 2) is an X509 v3 digital certificate [8]. 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, e.g. 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 Tag generation and revocation phases

In Figure 3 the tag generation revocation phases.

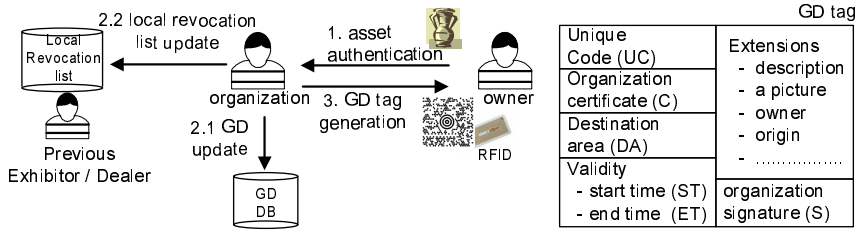

Fig. 3 The tag generation phase

In the tag generation phase an qualified organisation checks a cultural asset, if it is "authentic", the organisation generates a place and time based tag (GD) for it. A GD (see Figure 3) contains the following fields: (i) a Unique Code (UC); (ii) the organisation certificate (C); (iii) the destination area (DA); (iv) the starting time (ST); (v) the end time (ET); (vi) extensions; (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 section 3.1). The destination area field (DA) defines the location where the cultural asset will be exhibited/sold. The starting and end time denote the period in which the cultural asset will be exhibited or the period of the auction. The

[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.

extensions fields contains 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, in the CUSPIS project, 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.

The tag revocation phase is undertaken by an owner that wishes to withdraw its cultural asset from an exhibition/auction. To this aim the owner shows its GD to the organisation that reads it, verifies the signature *S* and checks the owner identity. If the GD is successfully verified then the organization updates the revocation list of the exhibition/auction where the cultural asset was destined for. In our implementation revocation lists are updated through a trusted logically centralised web site.

Organisations must take further measures to avoid a replication attack. A replication attack can result as a consequence of users asking for a new GD without revoking the old one. For instance if an owner has a two year tag, GD, for his cultural asset and he has lent it to an exhibition. Now suppose that the exhibitor uses the cultural asset to obtain a new tag, GD1, counterfeits the cultural asset and sells it to an auction. Then we are in a situation where two valid tags, at the same time, are used. Our approach is to require that organisations update and use a logically centralised data base of GDs. After an organisation authenticates a cultural asset it must query the DB with asset information [3]. In the case that a valid GD is currently issued then the organisation requires that the owner performs a revocation process. We emphasise that this is not the only solution to deal with the replication attack. For instance, if we assume that we have only short term GDs there is no need for both database and revocation lists.

Although cultural asset authentication requires organisations to have "cumbersome" tools, update a logically centralised DB and have specialised skills [10, 3, 4, 5], users can easily read all GDs and perform off line authentication with simple widespread devices (e.g., PDA).

3.3 The Authentication phase

In the authentication phase (see Figure 4), the end user reads a GD and verifies the authenticity of the related cultural asset. To this end the user employs mobile device

[2] We used RFID tags with 128KB of memory that maintain full compatibility with the EPC standard [9].

[3] In our current implementation, cultural asset search is performed based on the cultural asset type, period, weight and author. However, other techniques such as fingerprinting [10] are available to produce a unique ID for each cultural asset.

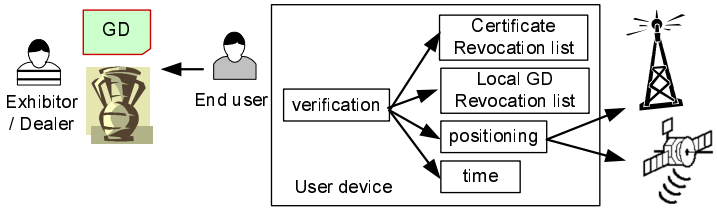

Fig. 4 The authentication phase

(e.g. a PDA) equipped with a verification component, a positioning component, two revocation lists and a time component. The main steps performed in the verification process are *replication checking*, *digital certificate verification*, *GD digital signature verification*, *place and time verification*, *object verification*, and *duplication checking*.

In the *replication 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 [8]. The public key of the certification authority and revocation lists can be downloaded from a trusted web site and installed prior to the verification.

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 *place and time verification* step, the verification component contacts the positioning component and the time component to get the user's current position and time. It is worth noting that the positioning component 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, in the CUSPIS project, the Authentication Navigation Messages (ANM) service [11] provided by Galileo satellite systems 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.

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

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. to perform 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 we are going to see in Section 5 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 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.

4 Security analysis

In this section, we provide a formal model of the system and discuss the security of our authentication system. Since the system is designed for special use cases, we do not intend to, and believe it would be difficult to, prove it is secure in a general settings. The security analysis in this section is bound to a specific context and certain assumptions, for example, in the analysis, we do not consider any attacks at the physical level, e.g. theft, destruction etc.

4.1 Modeling

The system is modeled as a tuple $(\mathscr{A}, \mathscr{A}', \mathscr{I}, \mathscr{C}, \mathscr{O}, \mathscr{P}, \mathscr{T}, \mathscr{CERT}, \mathscr{GD})$ whose elements are disjointed sets described as follows:

- $\mathscr{A}$ is the set of all cultural assets. $\mathscr{A}'$ is the set of counterfeit assets. $counterfeit : \mathscr{A} \to 2^{\mathscr{A}'}$ is a partial function. For a cultural asset $a \in \mathscr{A}$, $counterfeit(a) \in 2^{\mathscr{A}'}$ are the counterfeit items of a. $\mathscr{A}^0$ is defined as $\mathscr{A} \cup \mathscr{A}'$. $\mathscr{I}$ is the set of all identifiers. We also define a surjection mapping function $ID : \mathscr{A}^0 \to \mathscr{I}$, such that for all $a, b \in \mathscr{A}, a \neq b$ if and only if $ID(a) \neq ID(b)$ and for all $a, b \in \mathscr{A}^0, ID(a) = ID(b)$ if and only if we can find $x \in \mathscr{A}$ such that $a, b \in (x \cup counterfeit(x))$. Loosely speaking, this means that each real cultural asset has a unique identifier and the counterfeit items can be identified as the real asset.

- $\mathscr{C}$ is the set of all certification authorities in our system, i.e. the official departments. $\mathscr{O}$ is the set of all qualified organisations. Let $\mathscr{E} = \mathscr{C} \cup \mathscr{O}$, a function $pk : \mathscr{E} \rightarrow \{0,1\}^k$ defines the public key for each entity in $\mathscr{E}$, where k is a security parameter.
- $\mathscr{P}$ is the set of places. Function $in : \mathscr{P} \times \mathscr{P} \rightarrow boolean$ returns true if and only the first places lies within the second place.
- $\mathscr{T}$ is the set of times. Two times are comparable such that $t_1 < t_2$ and $t_2 > t_1$ if and only if t_1 is a time point before t_2, $t_1 = t_2$ if they refer to the same time point. $\leq, \geq$ are defined as abbreviations.
- $\mathscr{CERT}$ is the set of all valid certificates. Functions $subject : \mathscr{CERT} \rightarrow \mathscr{O}$, $issuer : \mathscr{CERT} \rightarrow \mathscr{C}$, $spk : \mathscr{CERT} \rightarrow \{0,1\}^k$ are defined to return the subject, the issuer and the subject public key field in the certificate. Function $certSig : \mathscr{CERT} \rightarrow \{0,1\}^m$ returns the signature of the certificate.
- $\mathscr{GD}$ is the set of all GDs created by the organisations. Function $getCert : \mathscr{GD} \rightarrow \mathscr{CERT}$ extracts the certificate embedded in the GD. Function $da : \mathscr{GD} \rightarrow \mathscr{P}$ returns the destination area. $validity : \mathscr{GD} \rightarrow (\mathscr{T}, \mathscr{T})$ returns the $(start, end)$ time period. $idInfo : \mathscr{GD} \rightarrow \mathscr{I}$ returns the identification information of the cultural asset stored in the extension field. Function $GDSig : \mathscr{GD} \rightarrow \{0,1\}^m$ returns the signature of the GD.
- For every public key key, key^{-1} denotes the related private key. Function $sign : \{0,1\}^* \times \{0,1\}^k \rightarrow \{0,1\}^m$ generates a signature over a message using a private key. Function $checkSign : \{0,1\}^* \times \{0,1\}^m \times \{0,1\}^k \rightarrow boolean$ checks the validity of a signature. $checkSign(m, sig, key) = true$ if and only if $sig = sign(m, key^{-1})$. We assume the cryptographic schemes are perfect. We also assume that each private key is only known by its owner.

With the model, we can formalise the authentication process in section 3.3 as shown in Fig. 5.

4.2 Proof sketch

For the sake of presentation, here we only sketch the proofs informally. The goal of authentication in our system is: given an asset a and a GD gd, current time t and place p, an authentication history in the period of the exhibition/auction $history$, decide whether the asset is real, i.e. $a \in \mathscr{A}$. It is clear that t, p and $history$ come from trusted sources and the attacker can manipulate the (a, gd) tuple. Let "real asset" denote $a \in \mathscr{A}$, "fake asset" denote $a \in \mathscr{A}'$, "matched tag" denote $gd \in \mathscr{GD}, ID(a) = idInfo(gd)$, "unmatched tag" denote $gd \in \mathscr{GD}, ID(a) \neq idInfo(gd)$,"fake tag" denote $gd \notin \mathscr{GD}$. Then there are six cases for the (a, gd) tuple: (i) a is a real asset and gd is a matched tag; (ii) a is a real asset and gd is a unmatched tag; (iii) a is a real asset and gd is a fake tag; (iv) a is a fake asset and gd is a matched tag; (v) a is a fake asset and gd is a unmatched tag; (vi) a is a fake asset and gd is a fake tag. Obviously, our authentication system is secure if the system returns $true$ only in case (i).

```
authentication((a,gd),t,p,history)
Output:
    true or false
Function:
    IF gdRevoked(gd)
        return false;
    ENDIF
    cert = getCert(gd);
    cSig = certSig(cert);
    issuer = issuer(cert);
    key = pk(issuer);
    IF certRevoked(cert)
        return false;
    ENDIF
    IF checkSign(cert,cSig,key)
        skey = spk(cert);
        gdSig = GDSig(gd);
        IF checkSign(gd,gdSig,skey)
            (t1,t2) = validity(gd);
            area = da(gd);
            IF t1 ≤ t ≤ t2 and in(p,area)
                id = idInfo(gd);
                IF id = ID(a)
                FOR EACH (gdi,pi) in history
                    IF gd = gdi and p ≠ pi
                        alarm();
                        return false;
                    ENDIF
                ENDFOR
                history = history||(gd,p);
                return true;
                ENDIF
            ENDIF
        ENDIF
    ENDIF
    return false;
```

Fig. 5 Algorithm for the authentication process

Now we will prove that our system is secure by enumerating all the possible attacks and show that they are either infeasible or not sensible.

It is easy to see that cases (iii) and (vi) are not possible. Under the assumption that the cryptographic schemes are perfect and only the owner knows the private key, the attacker cannot produce a valid signature for the forged or modified tag. The authentication returns $false$ in such cases. It is also easy to see that cases (ii) and (v) are not possible because the authentication will return $false$ in the object verification step.

Before going into case (iv), let's explain the intuitions of using position and time in our authentication system. The reason why we include position and time information is to limit the reuse/duplication of the tags. The underlying assumption of

the traditional certificate authentication is that the certificate is unique and is bound to the cultural asset. Unfortunately, in real life, the assumptions rarely hold. First of all, certificates can be duplicated, especially digital ones. Secondly, there is no way to bind the certificate to the asset directly, it can only be bound to the identification characteristics of the asset. This indirect binding makes the traditional system much weaker. For a cultural asset, the identity is easy to forge. The attacker can create a counterfeit item with the same appearance as the real asset. Then he can bind a recycled real certificate or a duplicated certificate to the counterfeit item in order to sell/exhibit them. Since the reuse/duplication can happen across a vast geographical-time space, the user cannot effectively track the usage of the certificate and detect the reuse/duplication. In our system, by using position and time as constraints, the tag is only valid in a specific area and a specific time period, so the attacker cannot use it or the duplicated ones in other places or other time. If the attacker reuses the tag or uses the duplicated ones within the valid place-time space, the reuse/duplication can be easily detected by the end user.

Returning to case (iv), given (a, gd), if the gd is issued to be used in another time or area, the place and time verification step will fail so it will be impossible to reuse a tag for other purposes. If the exhibitor/dealer uses a valid gd and binds it to different assets in the same exhibition/auction, the end user can detect it because the same gd will appear several times in the authentication history. Another possibility of case (iv) is that a valid gd is bound to a counterfeit item, but this gd is used only once in the exhibition/auction. In the exhibition case, the only entity who can do so is the exhibitor, but it is not sensible for the exhibitor to do so because if the tag is valid, it means the exhibitor has paid for the loan of the real asset and has permission to exhibit it in the exhibition. The exhibitor gains no advantage by exhibiting a counterfeit item while holding the real one. In the auction case, if the tag is valid, the asset bound to it must be real because the asset bound to the tag is authenticated and kept securely by a trusted party.

5 Implementation evaluation

Our system has been implemented and validated in the context of the CUSPIS European project [6]. 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. Exhibitions were organised in Villa Adriana (a roman villa), in the National Museum of Athens and in several places located in Rome.

In the case of Villa Adriana (an open space area) each cultural asset was equipped with an RFID device where the related GD is written. The destination area written inside the GD is an ordered list of points (i.e., a polygon) where each point is a couple of numbers (i.e., 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 location of a Roman sculpture inside Villa Adriana. Each user employs a mobile device equipped with both an RFID reader

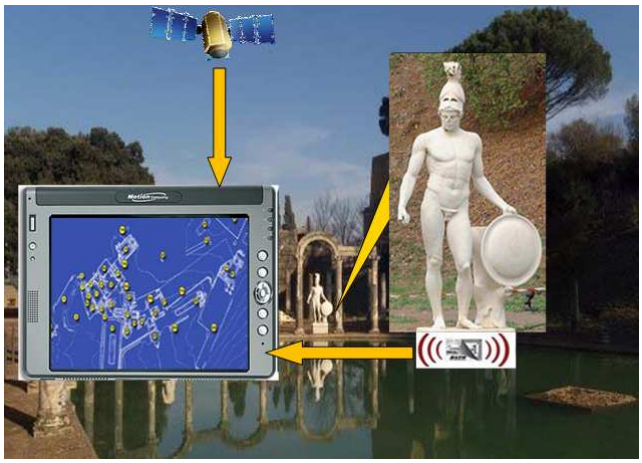

Fig. 6 A Roman sculpture exhibited in Villa Adriana

and a Galileo receiver. The mobile device reads the RFID information, a local key store, the Galileo time-positioning information, the authentication history and automatically checks the cultural assets authenticity. In particular the history authentication is used to check duplication as described in Section 5 by taking into account the range of our RFID tags. If the user reads the same tag GD in two different positions POS and POS' then when they differ more than the RFID radius range a duplication is found. It is worth noticing that within the RFID radius range the same GD will be quickly detected.

In Figure 6 we show part of Villa Adriana where the aforementioned sculpture is located. The sculpture's RFID is physically bound to its basement. On the left side of the picture we show the graphical user interface where the map of the villa is shown. This map shows the location of all cultural assets and the current user position. It is worth noticing that if the sculpture had been non-authentic a warning message would have been shown on the mobile device.

In the case of indoor exhibitions we have written a GD on a graphical code located next to its cultural asset. The destination area is encoded as a mail address (Roman temporary exhibition, via Dante Alighieri, n 34B, floor 2). People can take a picture of the code and receive all location and time information on their device. It is worth noting that in this case that the location verification is not automatic, a user has to read and validate the location data.

In Figure 7 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 [12]. In each museum mobile devices were used to locally perform the authentication of cultural assets in an efficient and fast way. Moreover, GDs with some variations have been used to transport and track cultural assets during their journey.

Our system has minimal cost for both organizations and for end users. Organizations 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 on a piece of paper. When GDs are written to RFIDs the organization must add the cost of the RFIDs. Users require a cellphone with RFID/GPS capability and a camera when GDs are stored as a graphical bar code.

Fig. 7 A picture displayed on the indoor visit

6 Related work

In this section we overview the related work in the area. We include systems supporting exhibitions; some because they present approaches to discourage imitations of valuable assets, others because they use place and time data for authentication purposes. We also consider RFID and graphical bar code technologies since they share our counterfeiting and integrity problems.

Systems with auto-localization functionalities are now available to help people visiting museums avoid traditional audio/visual pre-recorded guides. For instance, MAGA [13] 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 unique ID for the cultural asset. The ID is passed to the server application via a Wi-Fi connection 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 with in [14, 15] 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 mobile device can be easily copied and used for counterfeit assets.

ETG (Traceability and Guarantee Label) [16] 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 it provides data integrity it does not protect against the duplication attack since all encrypted data can be reused and copied.

RFID technology shares many of the counterfeiting and integrity problems [17]. Passive RFID have been successfully applied to identify, catalogue and track valuable assets [18, 19]. 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 [20]. 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 [17, 21, 22]. 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 organizations are trying to address it. For instance the EPC global standard for RFID technologies proposes global object naming services [23] that provide each object a with 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 still require time-space information to avoid duplication of asset information. In our approach although organizations coordinate to maintain a logically centralised data base of GDs, users perform offline GD verification thus scalability is enhanced.

In [24] 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). False alarm rate is reduced in the approach presented in [25] where they provide a probabilistic based approach for location based authentication. They use past location of products as location-based information for counterfeit asset detections. However, our system starts from different assumptions in fact very often previous locations of a cultural asset is unavailable but where it

will be exhibited is known a priori. Since we are dealing with high valuable objects no false alarm is permitted. Moreover, we have introduced different security measures (especially in the same destination area) to ensure security properties.

In [26] location information is used to address the forgery of origin information and the transport problems of assets [26]. Each asset is equipped with a tag that contains origin and tracking information signed with the producer 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 off line authentication verifications. We add the concept of time and authentication history to address the problem of duplication in the same area. Moreover, our approach is formally described and security properties are formally verified.

7 Conclusion and future works

Our place and time based system provides novel authentication and integrity services for cultural assets. Its main contribution is the combination of both place and time information as well as traditional security mechanisms to generate a place and time based tag for each cultural asset. This tag avoids duplication, reuse and modification of key cultural asset information. Moreover, it prevents the introduction of counterfeit cultural assets in the market. Our approach has been implemented and deployed in several museums where its performance has been validated by several users. As future work we are extending and generalising the use of place and time information to authenticate other kinds of assets (e.g., jewels, watches and wines).

References

1. Jacob, J.: Counterfeited arthow to keep it out of your collection:. Chub collectors (2002)
2. Center of Stuy TCI: Dossier of MUSEUM 2006 (2006) www.touringclub.it/ricerca/pdf/DOSSIER_MUSEI_2007.pdf.
3. BBC on line resource.: Radiocarbon Dating (2002) www.bbc.co.uk/ dna/h2g2/A637418.
4. Minnesota State University. : Thermoluminescence (2002) www.mnsu.edu/emuseum/ archaeology/dating/ thermoluminescence.html.
5. Klarreich, E.: Con artists: Scanning program can discern true art. science news **166** (2004) 340
6. European Commision 6th Framework Program - 2nd Call Galileo Joint Undertaking: Cultural Heritage Space Identification System (CUSPIS), (www.cuspis-project.info)
7. official web page of Galileo: (www.galileoju.com)
8. Stallings, W.: Cryptography and network security: Principles and Practice. Fourth edn. (2006)
9. web page on EPCglobal organization: (http://www.epcglobalinc.org/home)
10. James D. R. Buchanan and Russell P. Cowburn and Ana-Vanessa Jausovec and Dorothee Petit and Peter Seem and Gang Xiong and Del Atkinson and Kate Fenton and Dan A. Allwood and Matthew T. Bryan: 'Fingerprinting' documents and packaging. Nature **436** (2005)
11. Pozzobon, O., Wullems, C., Kubic, K.: Secure tracking using trusted gnss receivers and galileo authentication services. Journal of Global Positioning Systems **3** (2004) 200–207

12. (CUSPIS official home page, TITLE = CUSPIS demnonstration and performance avaluation report, p..w.)
13. Augello, A., Santangelo, A., Sorce, S., Pilato, G., Gentile, A., Genco, A., Gaglio, S.: Maga: A mobile archaeological guide at agrigento, (University of Palermo, *ICAR_CNR)
14. Pilato, G., Augello, A., Santangelo, A., Gentile, A., Gaglio, S.: An intelligent multimodal site-guide for the parco archeologico della valle dei templi in agrigento. In: Proc. of First European Workshop on Intelligent Technologies for Cultural Heritage Exploitation, at The 17th European Conference on Artificial Intelligence. (2006)
15. Park, D., Nam, T., Shi, C., Golub, G., Loan, C.V.: Designing an immersive tour experience system for cultural tour sites. In chi '06 extended abstracts on human factors in computing systems edn. ACM Press, New York, NY, 1193-1198, Montral, Qubec, Canada, April 22 - 27 (2006)
16. (web page of Italia Oggi journal) http://www.italiaoggi.it/giornali/ giornali.asp? codiciTestate=45&argomento=Circuits.
17. Juels, A.: Rfid security and privacy: A research survey. IEEE Journal on Selected Areas in Communication. (2006)
18. Caputo, T.: Rfid technology beyond wal-mart. WinesandVines (2005)
19. web page of the TagStream Company: (http://www.tagstreaminc.com)
20. Texas Instruments and VeriSign, Inc.: Securing the pharmaceutical supply chain with RFID and public-key infrastructure technologies., (Whitepaper, www.ti.com/ rfid/ docs/ customer/ eped-form.shtml)
21. Juels, A., Weis, S.A.: Authenticating pervasive devices with human protocols. In Shoup, V., ed.: CRYPTO. Volume 3621 of Lecture Notes in Computer Science., Springer (2005) 293–308
22. Tuyls, P., Batina, L.: Rfid-tags for anti-counterfeiting. In Pointcheval, D., ed.: CT-RSA. Volume 3860 of Lecture Notes in Computer Science., Springer (2006) 115–131
23. EPC global standard powered by GS1.: Object Naming Service (ONS) 5 Version 1.0, (Whitepaper, www.epcglobalinc.org/ standards/ Object_Naming_Service_ONS_Standard_Version_1.0.pdf EPCglobal Ratified Specification Version of October 4, 2005)
24. Mirowski, L.: Detecting clone radio frequency identifications tags. Bachelor's Thesis, School of Computing, University of Tasmania (2006)
25. Lehtonen, M., Michahelles, F., Fleisch, E.: Probabilistic approach for location-based authentication. In: 1st International Workshop on Security for Spontaneous Interaction IWSSI 2007. (2007)
26. Mostarda, L., Tocchio, A., Inverardi, P., Costantini, S.: A geo time authentication system. In proceeding of IFIPTM 2007, Joint iTrust and PST Conferences on Privacy, Trust Management and Security (2007)