A Geo Time Authentication System*

L. Mostarda, A. Tocchio, P. Inverardi, and S. Costantini

Dip. di Informatica, Università di L'Aquila, Coppito 67100, L'Aquila, Italy
{mostarda,tocchio,inverard,costantini}@di.univaq.it

In this paper we present Geo Time Authentication (GTA), a prototype system that provides authenticity and integrity of cultural assets information. It has been conceived in the context of the CUSPIS project and afterwards it has been generalized to the context of assets and goods where problems of counterfeiting and thefts are prevalent. To prevent these crimes GTA adds to the usual asset information an additional tag that contains Galileo geo time information and it extends digital certificates with the notion of geographical areas for protecting the origin and the authenticity of the assets. Moreover, GTA makes available several services to protect the assets transport.

1 Introduction

The painting of Jean-Marc Nattier, The Alliance of Love and Wine, 1744, synthesizes the core of this paper strangely. What do a certification of origin and an ancient picture where a man and a woman drink wine share in common? At first sight nothing but cultural assets and wine share a common risk: the possibility of being forged. High quality wines such as Barolo or Chateaux Bordeaux owe their fame to the geographic areas where vineyards are cultivated and wine is left to mature in casks. It is inconceivable to define Bordeaux as a bottle of wine coming from the Nero d'Avola vine in Sicily.

The assurance about the origin and the integrity of a wine is very important and for this purpose in France and in Italy the AOC (Appellation d'Origine Contrôlée) and DOC (Denominazione di Origine Controllata) certifications have been introduced. Their purpose is to protect the reputation of the regional foods and to eliminate unfair competition and misleading of consumers by non-genuine products, which may be of inferior quality or of different flavor. AOP, DOC and other certifications represent a relevant obstacle to the forgeries even if the problem of falsifying data as the geographical origin still remains. Generally speaking, the counterfeiting in the context of alimentary products presents two main branches: the faking of origin and the forgery of the producer. In Italy, in December 2006 the police operation "Nozze di Cana" sequestered a large quantity of low quality wine ready to be sold as Pinot grigio IGP, Prosecco e

* We thank the Next S.p.A. research group and the CUSPIS project partners. Their suggestions during the project meetings have improved the quality of this work. Moreover we thank Naranker Dulay who revised this paper

Please use the following format when citing this chapter:

Mostarda, L., Tocchio, A., Inverardi, P. and Costantini, S., 2007, in IFIP International Federation for Information Processing, Volume 238, Trust Management, eds. Etalle, S., Marsh, S., (Boston: Springer), pp. 123–138.

Pinot nero DOC. Moreover, it is estimated that in the U.S. the imitation of Made in Italy wine market is in fact almost equal to that which Italy exports. In other words, one out of two bottles of wine are "fakes" and it is easy to come across curious "Italian" bottles of Chianti, Sangiovese, Refosco, and Barbera, even Rosè, Barolo and Super Piemontese that are produced in California. Works of art share with wines the unhappy destiny to be stolen and faked. In Italy, the police operation "Canale" sequestered 20,000 pieces, paintings and graphics works, 17,000 of them were imitations. Works of art stolen belonged, mainly to religious places, houses and museums.

The main reason for the excessive development of this criminal activity is the absent or incomplete cataloguing of works of art and the inadequacy of passive defense systems. Moreover, even with good planning of the journey and an escort presence, sometimes the criminals are able to steal works of art in transit.

Is it possible to cut down the criminal activity on wine, works of art and other goods that ensure huge profits for few people to everybody's detriment? It is very difficult to find a definitive solution for this problem but a relevant role in the prevention of the criminal activities could be assigned to the Galileo satellite[2], a big brother capable not only of certificating the origin of products such as wine but also of following the works of art in museums and during their journeys. Our idea is to combine the Galileo services with public key certificates [12] in order to guarantee the producer, the origin and the destination of products such as wines, to authenticate works of art and to ensure the security in their transport. Both Galileo services and public key certificates have been combined in the Geo Time Authentication (GTA) system in order to enhance security services (i.e., identification, authentication, assets information integrity, secure transport) in the ubiquitous systems constituted by assets.

In the identification phase the Galileo services permit the tagging of an asset with a unique asset identification code (GAID) in which the Galileo coordinates have a relevant role. In particular, the Galileo Open Service (OS) [11, 10] provides to the GAID accurate positioning and timing information to uniquely catalogue an asset while the Galileo authentication service enhances the GAID with integrity and authentication information. GAID combined with 'extended' digital certificates (i.e., certificates that bind a producer to a geographical area) guarantees the precise origin of products and links the origin with the entity that produced them. In some cases it can also be useful to consider in the certification process the product destination. This concept can be applied more rarely to wines but in the context of the works of art transport, the destination authentication guarantees that people are looking at a genuine work in a museum or in a gallery of art.

Identification, authentication and secure transport of assets supported by the satellite could be a good response to the criminal phenomena emphasized earlier. GTA allows us to defend against the imitations of origin wines, dresses,

[2] Galileo is Europes own global navigation satellite system.

paintings and other products, allows people to check if an asset is in the place where it is destined to remain and, finally, allows museums to lend more easily works of art by considering the security guaranteed not only by Galileo but also by particular procedures of packing and control. Our approach has been developed and validated in the context of the CUSPIS project [5] by using the Galieo satellite but it can operate also with the support of other positioning infrastructures.

2 Defining the asset life cycle

In this section we introduce step by step the process that, starting by the producer, delivers assets to consumers. We call this process the asset life cycle. The life cycle is divided into four phases: (i) Certification; (ii) Identification; (iii) Transport; (iv) Selling and authentication.

Certification phase: In order to guarantee the traceability of an asset, a unique identifier (AID) must be assigned to it. This identifier is composed of two parts: the first one identifies the company (CI) while the second one is a serial number identifying a product of the company itself (PI). In order to generate the CI identifier, a company (i.e., the producer) can interact with some international organizations. The basic role of the international organizations is to guarantee the uniqueness of the CI. In the context of bar codes [3] in USA and Canada, this role is assigned to the GS1 (Global Standard 1) organization. When a company requests its CI from the GS1 and obtains it, the process of assets identification starts. The CI is joined to the asset serial number according to the Universal Product Code (UPC) standard and to the kind of asset. In fact a bar code does not distinguish among the same kind of assets. For instance, the same brand of wine with the same characteristics has the same bar code. A more promising technology is based on Radio Frequency Identifiers (RFID) [8] that holds both an asset unique identifier (AID) and the related description in a digital form. With respect to the bar code the RFID is able to identify uniquely an item.

Identification phase: In this phase the producer, after creating an asset, attaches to it Asset Data (AD). The AD contains both a description and the Asset Identifer (AID). The description is usually composed of some sentences that describe the product, the producer generalities and the origin (e.g., made in the USA). The AID uniquely identifies an asset and may allow a producer to perform easily an inventory, to verify the status of an asset by means of the tracking process and to oversee the correct assets management.

Transport phase: Transport is the step where products are packed and delivered by the transporter to the markets where they are sold.

Selling and authentication phase: In the selling phase the seller gets in touch with the consumer. The seller has assets equipped with ADs that are used for

[3] The printed code used for recognition by a bar code scanner (reader).

inventory purposes. The consumer can access the information in the AD for validating the product authenticity and capturing all data useful to determine the asset qualities and characteristics. The asset authentication process is usually performed by means of empirical rules, e.g., by looking at the description inside the AD and comparing it with the shape and the features of the product.

In the following we describe all attacks that can be performed on the asset description and on the AID (see [8] for a survey). Without loss of generality we will consider attacks that could be performed when the AD is stored on the RFID device. In fact, as we are going to see in the rest of the work, a basic RFID is more vulnerable than the traditional bare code [6].

3 Attacks on AD information

In the following we summarize the attacks that can be performed against an AD:

AD modification: An unauthorized entity can take the AD (i.e., description and/or AID) and tamper with it. This is an attack on the integrity of the AD information. In the context of the wine production and transport, either the carrier or the seller could modify both the AID and the description of a wine in order to change its data and/or its origin.

AD fabrication: An unauthorized entity can introduce counterfeit assets in the market. This is an attack to the authenticity of the product. For example in the field of the wines, an entity could produce a bottle of wine in Italy pretending that its origin was a vineyard located in France. A painter could create a copy of a famous painting and exhibit it as the original.

AD duplication: A malicious entity can duplicate a valid AD generated by an authorized producer. For instance, this is the case in which a malicious producer of wine duplicates AD data of a wine bottle and uses it on its bottles.

AD reuse: A malicious entity can reuse the AD information for other assets. For instance, a malicious producer can copy the AD information, destroy it and reuse the AD data in its product. A seller could misplace the AD from a bottle to another one or a museum employee could remove an ID from a work of art and put it on an imitation. A particular case of this general attack is the swapping one, in which an adversary exchanges two valid ADs.

AD destruction: A malicious entity can destroy the AD. For instance a malicious transporter can destroy the AD related to an asset.

AD access control An authorized entity can attempt unauthorized actions. In this case the device containing the AD must authenticate the AD reader in order to implement access control mechanisms.

Besides the security issues the RFID devices emphasize privacy issues since they do not require a direct line of sight and can be read without bearer authorization. For instance, EPC RFID contains a description field where the asset description can be stored. An attacker could capture information on products bought by a person, his clothing size and accessory preferences violating his

privacy. The producer can be affected by similar privacy violation acts. In fact, a competitor could be interested in acquiring information of his production methodologies and processes. This problem has been faced by the work of Juels et al. in [9]. Generally speaking clandestine tracking is a well-known problem that affects other devices such as Bluetooth or Wi-Fi (see [18] for an extended survey).

In order to design a secure system for the products having an AD we first have to define the notions of privacy and security; to this end, we have to know *against what* we want to be secure and private. Therefore, in the next section we will present a rigorous model of the attacks that an adversary can perform against the AD. Under this assumption we will identify interesting attacks that our Geo Time Authentication System is able to prevent.

4 The attack model

In our attack model we assume that an attacker: (i) can read (any number of times) an AD previously written; (ii) can rewrite an AD previously written; (iii) has its own instruments to fabricate an AD; (iv) can read the information flowing between an AD storage device and the related reader; (v) cannot interfere in the AD creation process, when a valid AD is created and stored in the related device by its producer.

In the following we consider the functionalities of AD storage devices (as we have emphasized in Section 2 we adopt RFID storage devices). Devices functionalities and asset life cycle characteristics will be used to validate the reasonableness and the correctness of our attack model. Finally, we provide some related work where other attack models are proposed.

RFIDs range from basic to advanced ones. Basic RFID devices cannot perform cryptographic operations, do not offer cloning resistance and can be easily read/written with a low-cost device. Advanced RFID devices offer some basic cryptographic operations, some form of cloning resistance, one-time writing and they implement basic access control mechanisms. In order to make our system as adaptable as possible we adopted basic RFID devices.

Concerning the asset life cycle, we observe that an asset identified by a producer can be handled by other entities during the asset life cycle. For instance a bottle of wine produced in France can be handled by the carrier that transports it in England or by the restaurant that serves it to the users.

The above considerations lead us to assume that an attacker can read, write, fabricate an AD information as emphasized in (i), (ii), (iii) and he can eavesdrop clear-text information sent between an RFID device and its reader (i.e., (iv)).

Concerning the assumption described in (v), it is consequence of two main considerations. First the supply chains of producers always provide some forms of physical security measures in the asset identification phase (see Section 2). Secondly there must be a physical proximity during AD generation. Therefore,

we can assume that a man-in-the-middle attack is not possible during the AD creation.

As described in [8], an important research challenge is the formulation of weakened attack models that accurately reflect real-worlds attacks in the field of AD and RFID devices. For instance in [7] a 'minimalist' security model for low-cost RFID devices is proposed. In this model an adversary can only read an AD on a periodic basis (and also tag release data at a limited rate). In particular, this model assumes an upper-bound on the number of times that an attacker can read the AD or spoof a valid AD reader. It is suitable for proximity cards where an adversary can only read the card. In the context of the asset life cycle, products are handled by different entities, for this reason the 'minimalist' model is not suitable. A more general model is proposed in [2] where all kinds of threats are described and related solutions shown. It has several characteristics in common with our model and this correspondence constitutes for us a validation of the model proposed in this paper.

5 The GTA system

The Geo Time Authentication (GTA) system provides security services in an ubiquitous context where assets equipped with digital devices are put everywhere. The GTA security services address: (i) authentication; (ii) access control; (iii) integrity; (iv) privacy and confidentiality; (v) secure transport of assets; (vi) non-repudiation. These services are countermeasure to the attacks described in Section 4.

The GTA authentication service guarantees the authenticity of an AD. This authenticity ensures that the producer is the one indicated on the AD and that the AD was indeed generated in the origin indicated on it. Moreover, AD authentication prevents an attacker from masquerading as a legitimate producer (more generally that counterfeit objects are introduced in the market). The GTA access control service is able to limit and control the access to the AD. To this aim each entity must be first authenticated so that access rights can be tailored to the individual. The GTA integrity service ensures that an AD is received as sent, i.e, duplication, reuse, destruction cannot be performed. The GTA privacy and confidentially services guarantee that AD information is provided only to authorized people. The GTA secure transport of assets ensures that assets are not stolen or substituted during the transport phase. The GTA non repudiation service prevents a producer to deny a generated AD. We will show that these services are implemented by using well known cryptographic mechanisms combined with Galileo service infrastructures and with the flexibility of the GTA configuration.

The GTA system can run in a completely decentralized configuration or with the addition of logically centralized components. In the decentralized configuration a user can easily use its mobile devices (e.g., a phone or a PDA) to locally check the authenticity and the integrity of an AD. For instance, in a

shop a user can verify the authenticity of a shirt without the need of any connection. The advantage of the decentralized solution is in terms of performance and scalability, i.e., an increasing number of users and assets does not affect the AD verification time. However, this solution does not provide access control mechanisms, privacy and secure transport of assets. In order to provide these services the GTA system relies on centralized components.

5.1 The decentralized GTA solution

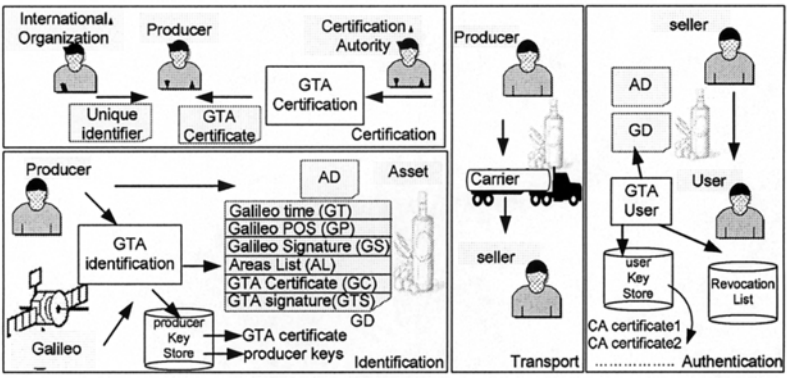

Fig. 1. The addition of the GTA components

In Figure 1 we show how the GTA decentralized solution is added in the asset life cycle. This addition does not affect the normal standard life cycle phases described in Section 2 since it only introduces certification authorities and an additional tag (the GTA tag (GD) shown in Figure 1) to each asset.

Certification phase. In the GTA system, different Certification Authorities (CAs) are equipped with the GTA certification component (see left-upper side of Figure 1). Each authority can release a GTA certificate to a producer. For instance in our application the Certifications Authorities are the Italian and Greek Ministries of Cultural Heritage and the Italian Commercial Entity (CCIAA). GTA certificates associated to museums are released by the Ministries while the Commercial Entity is involved in the generation of certificates for the producers of wine. A GTA certificate is an X509 v3 certificate[12] with the addition of GTA special extensions. A standard x509 v3 extension is a triple (*ID extension* ,*critical*, *extension Value*) used to store additional information in an X509 certificate. *ID extension* is an extension unique identifier. *Critical* is set to true (false) whether or not an implementation trying to process a X.509 certificate should be (should not be) able to understand the extension to correctly process the certificate. Finally, the *extension Value* field contains the data of the extension. For instance, the extension can be used to write in a certificate the Internet address where the List of Revoked

Certificates (CRL) can be downloaded. The GTA system uses the extension mechanism to store in a certificate a tuple (Description, Area) where *Description* is composed of some words that informally describe the field *Area* that is an ordered list of points (i.e., a polygon) identifying the place where products are built. For instance a GTA certificate can have the geographical extension $\{(FranceMargot, \{(46.290763, -0.839555), (46.286302, -0.816752), (46.277241, -0.820633), (46.282811, -0.847808)\})\}$ vouching that the producer bottles its wine in the square geographical area defined by the above points (i.e., France Margot). We point out that when a producer has different vineyards located in different areas, he must have different certificates, one for each area. This uniquely identifies uniquely not only the producer of the wine but also the geographical area where the bottle has been produced. In the case of cultural assets an area can guarantee the origin of cultural assets, i.e., where they have been discovered (e.g. Egypt) or the place where they have been authenticated (e.g. Louvre museum).

Identification phase. For each asset the GTA system adds to the standard AD the GTA Data (GD) (see left-lower side of Figure 1). To this aim each producer is equipped with a *GTA identification component.* This component takes in input the Galileo signal and the producer Key store where holds both the GTA certificate (obtained in the previous phase) and the public and private key of the producer. The component output is a GD for each asset. A GD contains the following information: (i) the Galileo time (GT); (ii) the Galileo position (GP); (iii) the Galileo Signature (GS); (iv) the Areas List (AL); (v) the GTA certificate (GC); (vi) the GTA signature (GTS).

The GP field corresponds to the geographical position (i.e., latitude, longitude and altitude) measured by a Galileo receiver[4]. The GT field is the Galileo time locally measured by means of a Galileo receiver. The use of GT and GP fields is twofold: from one side they are the GD part providing information on the time and on the geographical point where the asset has been created. On the other side they permit to uniquely identify each asset. In fact, we suppose that a producer can create in each instant only an asset and for each geographical point can exist only a producer. In the rest of this work the concatenation of the GT and the GP fields will be referred to as the Galileo Identifier (GAID). The GS is the Galileo digital signature of the GAID data. By using this digital signature, a Galileo receiver is able to authenticate the source of GP and GT data (i.e., the Galileo satellite) and verify their integrity[5]. Moreover, the GS ensures that a producer cannot counterfeit the origin of its product. The AL field defines a list of areas. These areas are useful for 'tracking' the product during its life cycle. For instance a wine producer can generate a list containing all 'destination' areas where the product will be sold, i.e., the areas identify-

[4] In closed environments the signal is forwarded from outside to inside by means of special devices.

[5] The Signal Authentication through Authentication Navigation Messages (ANM) is a Galileo service that will be active on 2008 [11]. In our GTA implementation integrity checking is based on cross-checking the Galileo signal.

ing a chain of restaurants. In the case of cultural assets the list can contain one destination area that identifies the museum where the cultural asset will be exhibited. The field GC contains the GTA certificate of the producer. The GTA signature (GTS) is a standard signature (SHA1 With RSA Encryption) of both GD fields (i.e. GAID , GS, AL, GC) and AD (if any) that is performed by the producer with its private key. This signature guarantees the integrity and authenticity of both GD and AD.

In the decentralized GTA implementation the size of a GD is about 1 Kilobyte and can been stored in both RFID devices [6] and bar code form. For instance in the case of cultural assets the RFID has been positioned next to each cultural asset in order to provide its authenticity. Concerning the bar code, it can be added in the label to the usual wine bar code to enhance security issues.

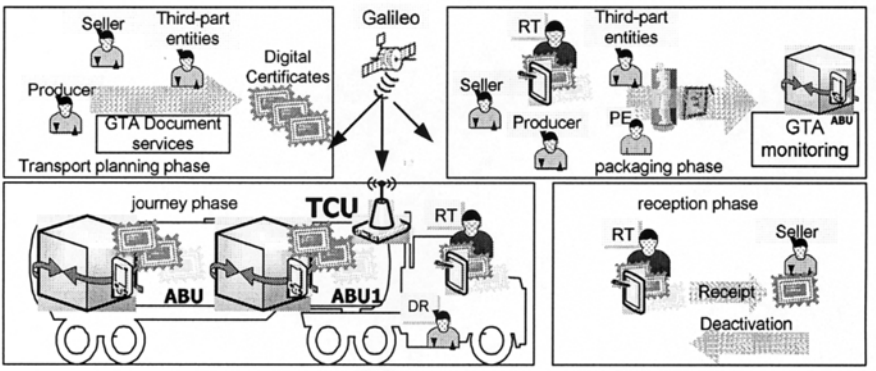

Fig. 2. The addition of the GTA components

Transport phase. In Figure 2 we provide a detailed description of the transport subphases: (i) transport planning; (ii) packaging; (iii) journey; (iv) reception.

In the transport planning phase different entities use the GTA document services component in order to produce different certificates. Entities are the producer (i.e., the owner of the asset), the seller (the entity who wishes to take the assets) and third-part entities (i.e., who vouches the content and the routing of transport). In particular, digital certificates must include an authorization certificate for each package and a unique transport certificate. Each authorization certificate can contain the list of all GDs inserted in the package. The transport certificate contains the correct routing. The routing of the transport certificate 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 starting transport area and T_{A_s} the related date (i.e., day and hour), A_i an area at which the transport must pass and T_{A_i} the related date, (A_d, T_{A_d}) the destination area and its date.

[6] There are RFID tags with this size that maintain full EPC compatibility.

We point out that for specific assets transport other certificates (e.g., insurance certificates) can be added, moreover all certificates are signed by all entities. For instance in the context of CUSPIS project we have transported cultural assets. In this case the producer is the owner of the cultural assets, the seller is the renter of cultural assets and third-party entities are the Ministry of Cultural Heritage, the Insurance Company and the Transporter. Those entities cooperate to produce the above digital certificates (i.e., the authorization certificates, the transport certificate and the insurance certificate).

In the packaging phase the above entities in cooperation with a transporter (RT) and the packaging expert (PE) supervise the packaging of assets. Each package is filled with: (i) a set of assets each identified by an AD and the related GD; (ii) an Asset Board Unit (ABU); (iii) a sensor of humidity; (iv) a sensor of light; (v) a sensor of temperature. The ABU is equipped with a GTA monitoring component, the authorization certificate related to the package, the transport certificate and additional certificates.

The journey phase starts with a startup message that the transporter sends to all ABUs. Each ABU verifies: (i) the transporter identity; (ii) the correct starting position; (iii) the presence of all GDs in its package . Moreover, each ABU gathers all distances from other ABUs and all sensors data. During the journey each ABU checks that both sensors data and the ABUs distance do not vary. The former check ensures that packages are not opened while the latter that packages are not stolen. Correct routing is enabled by the Galileo signal used by each ABU in order to check that all areas are passed at the correct time. In the context of CUSPIS project we have transported cultural assets from Rome to Florence (see the CUSPIS [5] project for details).

In the reception phase the transporter sends a reception message to the renter. This renter receives this message and sends a deactivation message to all ABUs. In particular each ABU deactivates its GTA monitoring system component only when it is in the right area (i.e., the destination area), the renter provides a valid certificate and the receipt is correctly formatted.

Authentication phase After the identification phase the assets are delivered to the market where their authenticity will be verified by a user. To this end the user mobile device is equipped with a GTA user component (see right-side of Figure 1) that is able to check the authenticity and the integrity of both the GD and the AD. A GTA user component interacts with a local user key store and a local revocation list. The user key store contains the digital certificates of all valid certification authorities. The revocation list should be updated as often as possible and it contains all GTA certificates that have been revoked. In order to check a GD and AD the GTA component performs the following steps:

- *GTA certificate (GC) verification.* This step involves the usual verification performed on x509 certificates [12]. In the following we describe the most relevant verifications that are performed. The certificate expiration date and its period must be validated. The issuer (i.e., a certification authority) who released the certificate must be a valid one (i.e., present on the local user

key store). The GTA certificate signature, which includes signature of subject name (i.e., the producer) and subject key, has to be checked w.r.t. the certification authority key. The GTA certificate must not be present in the certificate revocation list.

- *Galileo signature (GS) verification.* The Galileo signature (GS) must be verified w.r.t. both the Galileo position (GP) and the Galileo time (GT).
- *Origin verification.* This step verifies that the origin of the product (the Galileo position (GP)) is contained inside the area defined in the GTA certificate.
- *Actual position verification.* This step checks if the actual asset position belongs to the area defined inside the areas list (AL) present in the GD.
- *GTS signature verification.* This step verifies that the signature of both AD and GD data is correct (w.r.t. the producer public key contained in the GTA certificate).

In the following we will see that the GD and the AD can be used in order to address the attacks presented in Section 4 (i.e., to provide the GTA services described in the first part of this section).

The GTA authentication services rely on the GTA certificate (GC) verification step and on the Galileo signature (GS) verification. The former guarantees the 'authenticity' of the producer and the latter the origin of the product. The GTS signature guarantees the GTA non-repudiation service since it is based on asymmetric key technology. Moreover, the GTS signature even ensures detection of the AD and GD modifications (i.e., an aspect of the integrity service).

AD and GD reuse and duplication (i.e., the remaining attacks avoided by the integrity service), are addressed by the actual position verification step and/or by the use of a distributed GTA integrity component. The actual position verification ensures that the asset stays in one of the areas included in the GD areas list (AL) so that reuse (i.e., misplace and swapping) and duplication of AD and GD is bounded. In fact, a faked product should be distributed in the same restricted area where the original one resides. For instance suppose that a malicious producer reads the GD and AD of a famous wine in a market of New York in order to put them on a bottle of low quality wine. He cannot duplicate and reuse the GA and AD information in its falsified bottle. In fact, the purchasing of it in a place different from the original destination (e.g., a market of S.Francisco) will be detected by the GTA system through the actual position verification. But, the problems of reuse and duplication in the same area still remain. To address this we introduce the following solutions.

In the same area, swapping and misplacing are under the judgment of a user. We assume that the AD and GD information, received in the GTA user terminal, are coupled with a user's careful asset 'observation'. Observation can include the checking of the AD (e.g., the label information and the bar code), the shape and the form of the asset. For instance a GTA user can receive information on its terminal about a bottle of wine (i.e., the label, the form and the features of the bottle) and identify a possible misplacing or swapping of both AD and GD. Another solution to the reuse threat is to secure physically both the AD and

the GD. For instance in a museum both AD and GD should be secured next to the cultural asset in such a way that no unauthorized person can access it. Concerning the duplication prevention it can rely either on GD and AD storage devices (for instance actual RFIDs are equipped with anti-cloning devices [8]) or on a decentralized GTA system integrity component. Each area can have associated a centralized GTA integrity component which is based on a local GTA database. The asset GAID is a unique handler to the local GTA database where are stored information related to the asset purchasing data (i.e., whether or not the asset has been bought). Every time a user authenticates an asset, an enhanced GTA user component forwards the asset location data and the GAID to the GTA integrity component. The GTA integrity component checks if the AD is related to an asset never bought and raises an alarm when both AD and GD have been already checked out. It is worth noticing that the AD duplication is guaranteed by the singleness of each GAID code.

However, in real industrial context it is not always possible to generate GDs that contain the areas list (AL) information. Moreover, unless storage device are equipped with cryptography and access control mechanisms, both AD and GD information are visible and accessible to any user. In order to enhance these security and privacy issues the GTA system provides the following centralized configuration.

5.2 The GTA centralized solution

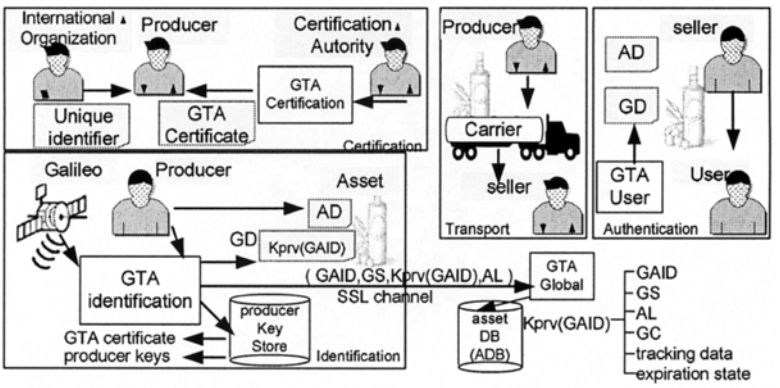

Fig. 3. The addition of the centralized GTA component

In Figure 3 we show how the GTA centralized solution is added in the asset life cycle. As for the decentralized solution the centralized one does not affect the asset life cycle phases but incorporates only a new centralized component, the GTA global component. This component is implemented in terms of different sub-components (see the online official CUSPIS documentation [5] for details)

that interact with each other in order to provide the GTA security services. In this paper, for space reasons, we do not describe the sub-components view but we merely consider the GTA global component as a black-box one. It is worth noticing that, as we are going to see in the phases description, both the GTA identification and the GTA user components are named as the ones described in the previous section but they are based on a different implementation.

Certification phase The certification phase is not modified with respect to the previous Section since a producer must still obtain its certificates in the same way.

Identification phase For each asset the GTA system adds to the standard AD (if any) the GTA Data (GD) (see left-lower side of Figure 3). To this aim each producer is equipped with a *GTA identification component.* This component takes in input the Galileo signal and the producer Key store and outputs a GD for each asset. A GD contains the GAID (i.e., Galileo time and the Galileo position) encrypted with the producer private key (this is denoted with $k_{priv}(GAID)$ in Figure 3). After the GD information has been produced the GTA identification component creates an SSL connection (mutual authentication is obtained through digital certificates) with the Global GTA component. This connection is used to transfer both GD data and additional asset data (see Figure 3). Additional data are those described in Section 5.1, the GAID, the areas list AL (if any) and the Galileo signature (GS) (see Figure 3). The global component stores the received data and some additional ones in the assets database (ADB). Additional data are the GTA certificate of the producer (GC) and the tracking and expiration ones. The tracking data contain a list of points where the asset has been observed. The expiration state can be set to 'killed' when the asset information has expired[7].

Authentication phase. After the identification phase the assets are delivered to the market where their authenticity will be verified by a user. The user mobile device is equipped with a GTA user component (see right-side of Figure 3) that is able to check the authenticity and the integrity of both an AD and the related GD. The GTA component sends the GD (e.g., $k_{priv}(GAID)$), the user position (e.g., Ux,Uy) and the related Galileo signature (GS(Ux,Uy)) to the GTA global component that performs the following basic steps:

- *User data verification.* The integrity of the user position is checked by using the Galileo signature GS(Ux,Uy). Moreover, there must exist an ADB entry labeled with key $k_{priv}(GAID)$.
- *Access control verification.* An access control component verifies the user rights in order to provide the asset data.
- *Expiration checking.* The entry $k_{priv}(GAID)$ must not be related to an asset expired.
- *Actual position verification.* The user position and its asset tracking data are matched to verify whether or not the user is looking at the original asset or

[7] For instance, an asset information can expire as a consequence of checkout

a duplicated/reused one[8]. Moreover, if the areas list of the asset is available (i.e., the possible asset locations) then it can be used to validate the correct asset location.

The GTA authentication service is based on the user data verification step where the GTA global component uses the $k_{priv}(GAID)$ handler to guarantee the existence of a valid asset entry. The $k_{priv}(GAID)$ signed handler even guarantees the GTA non-repudiation service since it is based on the producer private key.

Both AD and GD modification (i.e., an aspect of the integrity service) is guaranteed by the user data verification which checks the existence of the entry $k_{priv}(GAID)$. The AD and GS reuse/duplication (i.e., the remaining attacks avoided by the integrity services), are addressed by Expiration checking and Actual position verification steps. In the case that the asset expiration data is set to killed the GTA system detects that the asset could be reused. The actual position verification discovers when the asset is in an anomalous position or appears in too many different geographic positions. This check would allow duplications to be detected.

The GTA global component provides access control mechanism, for instance in the case of cultural assets information a user can get them only when they are paid for. For wine a user can get information only when the product has not been destroyed. Furthermore, the GTA system addresses the problem of AD and GD destruction by means of the time-out that expires when a product is unused for too long. The privacy in ensured by the encrypted GD which does not provide asset information.

6 Related work

In this section we cite some systems that face the problem of the origin certification or the secure transport of assets. Some can be compared because they are used to discourage imitation, some because they are based on RFID technology, others because are supported by the Galileo services. In the context of the origin certification, we cite the ETG [14] a system presented recently in Vicenzaoro Winter, capable of defending products against the problem of imitations. ETG (Traceability and Guarantee Label) supports the automatic printing and the reading of informative messages, based on a encrypted bar code. RFIDs have been applied successfully in the context of wines and is reported in WinesandVines, a trade publication for the grape and wine industry [3]. Some wineries adopted RFID tags for tracking data on individual barrels and tanks. For example, Barrel Trak [16] is an advanced process data management system that brings real time, read/write data tracking and process history to the winemaking process. RFIDs containing non-encrypted information are useful for maintaining track of the wines bottles in restricted environments as

[8] A similar technique is used for to detect possible credit card cloning.

wineries or restaurants but, what happens if the products of a winery are numerous and exported all over the world? The possibility of duplicating or faking an RFID increases considerably. The support of Galileo in GTA permits the introduction in the bottle identification code of information on the geographical area where it has been bottled. The concept that we intend to emphasize is that the RFID in GTA contains the coordinates where the products has been realized, so increasing the difficulties for faking it. In fact, in the case of the Barrel Trak, a bottle of a forged wine could be equipped with an RFID created in Europe vouching that the product has been bottled in California. Contrary, with GTA for faking the information in a RFID the falsifier should create it in the same geographical area of the Barrel Trak. This decreases the imitation probabilities. A good survey on the techniques for augmenting RFID security and security is [8]. Juels explores several methodologies for avoiding RFID duplications and tampering but none of them use the Galileo signal in order to enhance security issues. Galileo can take on a basic role to ensure the singleness, the authenticity and the origin of the RFID information considering also its relevant role in the information encryption process. RFIDs and cultural assets share the scene in the work of Augello et al. [1]. MAGA is a user friendly virtual guide system adaptable to the user needs of mobility and therefore usable on different mobile devices (e.g. PDAs, Smartphones). In MAGA RFIDs are applied to furnish information to the user but it is not clear if the authors faced the problem of the identification and authentication of cultural assets. In the context of Galileo applications (Agriculture and Fisheries, Civil Engineering, Energy, Environment and so on) [10], GTA confirms its originality in facing the problem of identification, authentication and secure transport of products. Two companies, Texas Instruments and VeriSign Inc., have proposed a 'chain-of-custody' approach that is strictly related to the GTA system [13]. Their model involves digital signing of tag data to provide integrity assurance. Digital signatures do not confer cloning resistance to tags, however. They prevent forging of data, but not copying of data. The EPC global standard for RFID technologies proposes global object naming services [4]. A centralized database stores assets information and can be used for security purposes. The GTA system enhances this with the notion of areas and the Galileo infrastructure. In particular, in the decentralized solution the security services are provided through local databases that do not need any data exchange. Therefore, performance and scalability are enhanced.

7 Conclusions

The GTA system provides novel security services in an ubiquitous system made of assets and the related devices. The combination of both Galileo services and enhanced digital certificates prevents counterfeiting of origins and the introduction of false assets in the market. The GTA limits duplication and reuse of assets information in the same geographical area where a local database can provide a

solution. The flexibility of its configuration permits the tuning of the system as needed. For instance when privacy is a relevant concern the centralized solution can be used. In contrast when scalability and performance are relevant concerns the decentralized solution can be applied.

References

1. 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.
2. Bailey D. and Juels A (2006) Shoehorning security into the EPC standard. In: De Prisco R, Yung M (eds) International Conference on Security in Communication Networks, volume 4116 of LNCS, pages 303–320, Springer-Verlag.
3. Caputo T. (2005) Rfid technology beyond wal-mart. WinesandVines.
4. EPC global standard powered by GS1 (2005) 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.
5. European Commision 6th Framework Program - 2nd Call Galileo Joint Undertaking. Cultural Heritage Space Identification System (CUSPIS). www.cuspis-project.info.
6. Garfinkel S and Rosemberg B (2005) Hacking the prox card. In: RFID:Applications,Security and privacy, pages 291–300. MA: Addison-Wesley.
7. Juels A (2004) Minimalist cryptography for low-cost rfid tags. In: Proc. 4th International Conference on Security Communication Network, C. Blundo and C. Blundo, Eds. New York: Springer LNCS.
8. Juels A (2006) Rfid security and privacy: A research survey. IEEE Journal on Selected Areas in Communication.
9. Juels A, Molnar D, and Wagner D (2005) Security and privacy issues in e-passports. In: Gollman D, Li G, Tsudik G, (eds) IEEE/CreateNet SecureComm.
10. official web page of Galileo. www.galileoju.com.
11. Pozzobon O, Wullems C, Kubic K. (2004) Secure tracking using trusted gnss receivers and galileo authentication services. Journal of Global Positioning Systems.
12. Stallings W (2006) Cryptography and network security: Principles and Practice. Fourth edition, Prentice Hall (eds).
13. 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.
14. web page of Italia Oggi journal. www.italiaoggi.it/giornali/giornali.asp?codici Testate=45&argomento=Circuits.
15. web page of the Sea Smoke Cellars. www.packagingdigest.com/articles/200509/ 64.php.
16. web page of the TagStream Company. www.tagstreaminc.com.
17. web page on EPCglobal organization. www.epcglobalinc.org/home.
18. Jakobsson M and Wetzel S (2001). Security weakness in Bluetooth. volume 2020 of LNCS. Springer Verlang.