A safe antifraud system for art: SafeArt

GIOVANNI NERI and MATTEO ARTUSO
Dipartimento di Elettronica Informatica e Sistemistica
Università degli studi di Bologna
Viale Risorgimento 2 – 40136 Bologna
ITALY
giovanni.neri@unibo.it matartuso@gmail.com http://gneri.deis.unibo.it

Abstract - It is well known that the world of art (paintings, sculptures, graphics etc) is plagued by the virus of counterfeits and this issue is particularly sensible in a country like Italy where art has flourished for centuries and where in the XX century too many pieces of art of great painters were copied and/or counterfeited and sold for authentic. Counterfeiting is a crime which involve great amounts of money and is perpetrated at all levels, with no exclusion of the greatest art dealers. Once a style or painter has had success it is even too simple to find a epigone which either can copy a single painting or paints according to one particular style. Great examples in Italy are Morandi, De Chirico, Vedova etc. artists with a well defined (and therefore easy to copy) style. In our university we have developed and implemented a digital system which can prove without any doubt the authenticity of a piece of art and which is tamper-proof at all levels.

Key-Words: - Art authenticity, digital signature, wireless devices,

1 Introduction

First of all it is must be understood what art counterfeiting means [1],[2],[3]. There are obviously two major fields: old pieces of art of dead artists and those of living artists. In this paper we refer with a general meaning to "pieces of art" which can be of any type (paintings, sculptures, graphics etc). Let's first of all describe the counterfeiting techniques which are generally employed. A typical fraud is the copy, sold as original, of a masterpiece of a private collection with an official "expertise" of a complacent "expert" who is an active part of the fraud. People should not forget that paintings are not sold only in auctions (where this type of fraud is very or less likely) but very often and mainly by private dealers and the a single "sting" can fetch tens or hundreds of thousand dollars. We had a just a case in Bologna two years ago with a Morandi's "Still life" (with the typical bottles) like that of the figure 1 (not the same) sold as authentic while it was only a bad copy of the original painting with thousands of Euros involved. This fraud is also very often perpetrated by the family of a deceased painter by validating for money a non original painting on the ground that they are the only real authoritative source of information and that they kept some of the painting unpublished.

Fig. 1

Another fraud of the families of painters, similar to the latter, is the case of the "post mortem" (after death) paintings. In this case the family of a painter asks the dying painter to sign some blank canvasses on which someone else will later paint in his style: the signature is authentic, the painting is not !!

(This raises a very difficult question: what is a piece of art for ? Beauty, pleasure or financial exploitation ? Why authenticity is more important than beauty ? Why a Picasso pencil hieroglyphic on a paper towel has a value thousand times higher than a full portrait of a good but less notorious painter of the same period ?). As far as the paintings of the past and/or of dead artists are concerned it is quite clear that people can only rely on trustworthy and experienced experts (who however very often make unwanted mistakes with thousands of dollars at stake) and this means that for each single piece of art there should be only one "official" expertise possibly recorded in a well maintained data base, as that of Museums, Galleries etc. But what for the pieces of art sold on the free market ?

A very interesting and promising mathematical approach is provided by the studies of Rockmore and others [4] whereby a the characteristics of a canvas under investigation are compared with the style characteristics of an absolute original canvas of the supposed same author and a confidence curve is derived. Good results were achievef during the investigations of Pietere Bruegel the Elder, a painter particularly beloved by counterfeiters. In our case we take a different approach and tackle a different problem: the absolute authenticity of new pieces of art and the authenticity of the expertises of old pieces of art, This means that there must be an absolute safe system which *links* the expertise - either done by the living author *once the piece of art if completed* or performed by a group of official experts and the piece of art. Safeart addresses this problems.

2 Digital signature

Digital signature is based on the RSA algorithm [5] or the so called "two keys system" which exploits devices able to producing two different but linked keys, one private (internal to the device and irretrievable) and the other public. Documents are signed with the private key (secret) and the signature can be checked against the public key which is normally published on web sites. Basically the security of the entire system is based on the fact that decomposition of a number in prime factors (in this case very very large number – 1024/2048/4096 bits) is a *np-complete* procedure whose cracking would requires tenths of years to all computers of the world. In Europe in 1999 a directive was approved [6] which states that the digital signature should prospectively substitute the personal signature in all official documents: this directive had be transformed in a law by the single members of EU. When this directive was approved Italy had already a law for digital signature which in many cases was far better and compelling than that of the EU commission which favored more the market competition among companies. Italy has already accepted the directive and we have a comprehensive law:

*(Codice della amministrazione digitale - www.**cnipa**.gov.it/site/_files/Opuscolo%2013II.pdf)*

and a regulatory body (CNIPA). Digital signature has three very important characteristics: it grants that a digitally signed dematerialized document (a file) is *original* (that means that no single bit was altered after the digital signature), it links the *identity* of the underwriter to the file and provides an official time stamp (unalterable too otherwise the digital signature verification fails) which legally determines the exact *time* when the document was signed. Moreover a single file can bear more than one digital signature. These characteristics can be fruitfully exploited to combat the counterfeiting. If it is possible to link in an absolute safe mode the piece of art and a digitally signed expertise file the problem could be solved.

3 Safeart system

We have exploited the wireless technology for the solution of the problem. There are today contactless wireless chips which can be connected to a PC and which handle the digital signature procedure (key generation and document hash signature). Let's first of all consider the case of a living artist. Once he has finished his piece of art he can photograph it, describe it, take a picture of himself near the item and so on: he can therefore build a file with all possible informatio which must be safely linked to the piece of art. We have used this devices (which are produced by several electronics industries) and a very special glue to glue the device to the piece of art which on one hand prevents the removal of the device without damaging the canvas or any other used material, and on the other hand does not damage the electronic device. Once the wireless device has been glued to the canvas (or any other material) the PC issues a command to the device which upon receiving it produces the couple of keys: the secret key (safely stored in the chip) and the public key which is communicated to the PC. The file with the information previously described is then completed with the addition of the public key received from the device and signed by the artist with his digital signature and the *official time stamp* (see figure 2).

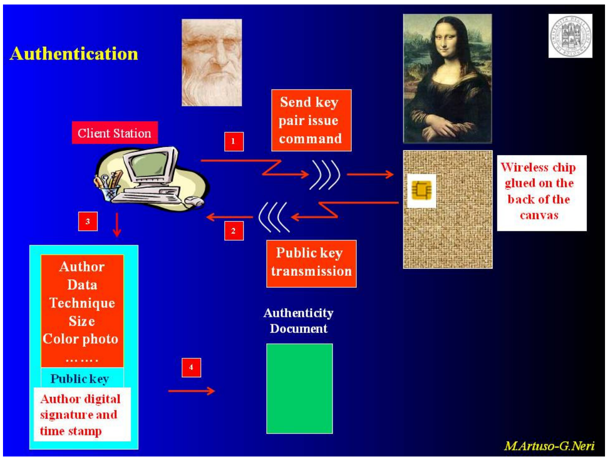

Authentication
Client Station
1
Send key pair issue command
Wireless chip glued on the back of the canvas
2
Public key transmission
3
Author
Data
Technique
Size
Color photo
……
Public key
Author digital signature and time stamp
4
Authenticity Document
M.Artuso-G.Neri

Fig. 2

When the authenticity of a painting must be verified it is enough to bring a PC with the signed file and its transmitter/receiver in the vicinity of the piece of art. The signature of signed file is first checked, then a short challenge message is sent to the device which in turns signs it with its private key. The final step it to check the correctness of the signed challenge using the public key of the device previously inserted in the already signed (by the artist) file. If the test is Ok then we are sure that the painting is undeniably linked to the file (which has been in no way tampered – [7]) and therefore authentic). In the following figure 3 the procedure is graphically explained which in the following paragraphs will be described in detail..

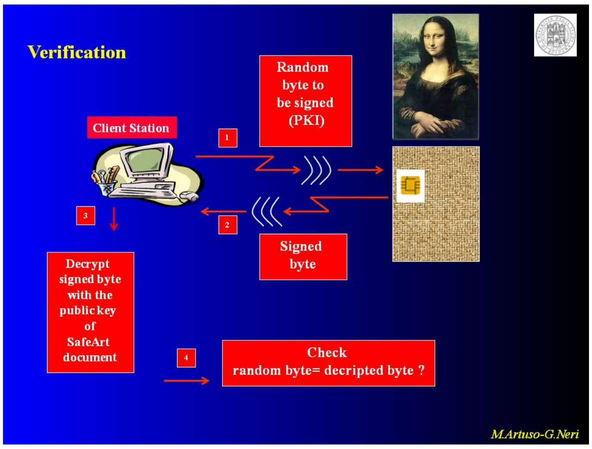

Verification
Client Station
1
Random byte to be signed (PKI)
2
Signed byte
3
Decrypt signed byte with the public key of SafeArt document
4
Check
random byte= decripted byte ?
M.Artuso-G.Neri

Fig. 3

Obviously the security of the system does not rely *only* on the digital signature technique used in the PC and on the chip but also on the protocol for exchanging information between the wireless chip and PC. To this purpose we must remember that a safe protocol has been standardized for the contactless cards - in this case only the glued chip - (ISO 14443) for contactless smart cards operating in close proximity with a reader antenna so as to create interoperability for contactless smart products. Both devices, reader and contactless chip, have to be compliant with ISO 14443, Identification Cards standard series which is made of four sections:

1. Physical Characteristic (part 1).
2. Radio frequency, power and signal interface (part 2).
3. Device initialisation and anti-collision (part 3).
4. Transmission Protocol (part 4).

All these sections are related to the two main communication protocols for proximity devices, Type A and Type B. Physical and radio sections set the electronic circuits characteristic for physically connecting devices. Initialization and anti-collision define the rules to prevent data block switch between different proximity chips connected to same reader. Transmission protocol regards the data communication by defining the protocol state machine and the logical meaning of each bits data block exchanged between reader and chip. Transmission protocol is mainly divided into three phases:

1. Handshake, where reader and chip define commands and parameters format they will use during data transfer.
2. Exchange data block of information. According to handshake, reader could send command to chip and exchange information with It.
3. Close of communication. At the end of transmission data chip has to be deselected from reader.

Data exchange between reader and proximity chip, technically called APDU (Application Protocol Data Unit), is described by ISO 7816-4 and more completely by ISO 7816 [8] that cater for "secure messaging" and "cryptographic tokens".

The aforementioned standards define all possible electronic and communication characteristics. To the signed document all possible variations can be applied as far as the number of signatures, the type of information etc. is concerned. The stored information will be heavily dependent on the nature of the type of art, be it visual, multimedial, graphic etc.. In this case it is only the fantasy of the artist the limit of the content and the degree of security which he wants to reach. It is obviously clear that the same identical procedure can be applied to old pieces of art. In this case we speak of "expertises" but the procedure is 100% identical with the only difference that the signature will not be that of the author but that of the expert (or of the experts) who certifies the authenticity of the item, its author and so on. There is also a further degree of security. Digital signature can only certify that the card used for signature was that of the author and that the signature was performed at a particular time. In order to be sure that the card *was used* by the artist a biometric-like system must be used. Among the possible means we use in Italy the so called "firma autenticata" (certified signature) : on top of the signature of the artist another digital signature is added, that of a notary (an officially recognized person for certifications) which upon ascertaining the identity of the signing person (by means of an identity card, knowledge of the person etc) adds his signature to the file as a proof of the identification. According to the laws of each single country it is in any case possible to implement such high level of security. The entire procedure has been implemented using a web interface and java language.

3 System architecture

In figure 4 a possible system architecture is presented.

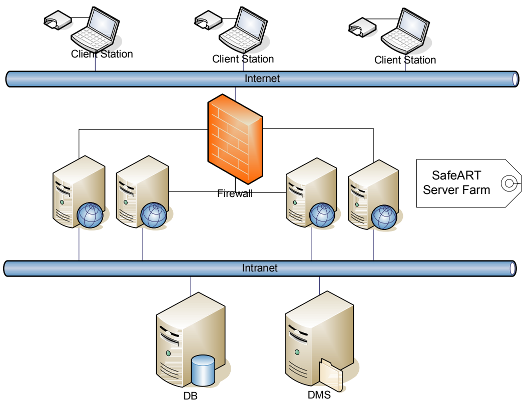


Fig. 4

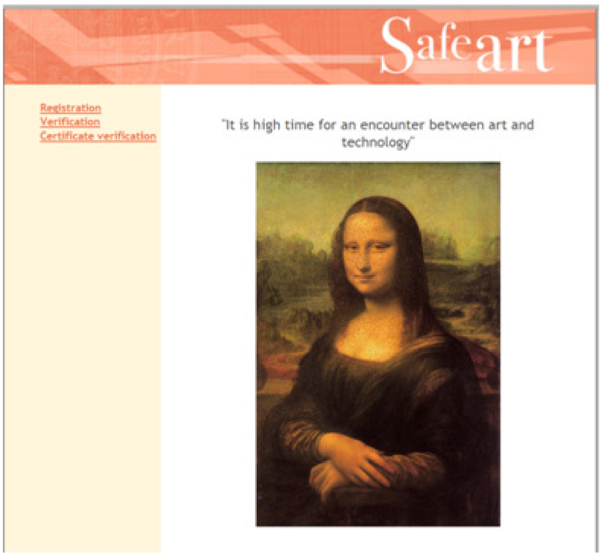
The computers are normal PCs (desktop, notebook or netbook) with network links, smart card readers (often integrated in the PCs) and a wireless smartcard reader (which can be used by through a USB interface). The browser of the PCs requires a java support. The servers can be tailored to the needs of the certification network. They must have a DB system in order to store the data of the registered pieces of art and of the users. The DB should be also synchronized with a DMS in order to archive the digital documents related to the registration, for instance for already existing items certification. There are two main "actors" in the system: Author and Certifiers.

4 - Certification

The Certification process follows these steps:

1) Author registration (if not already in the system DB)
   a. Identification data (date and place of birth, residence, age etc.)
   b. Unique code assignment

   c. Registration and association of a digital signature through a SmartCard
2) Art item information collection
   a. Photographs
   b. Used technique
   c. Materials (type of canvas, colors etc.)
   d. Other relevant information
3) Wireless chip gluing (canvas, marble etc.)
4) RSA keys pair generation through Smart cart proximity protocol (ISO 14443)
5) RSA keys pair generation which will form the property certificate and which will given to the proprietor
6) File creation which stores all data described in point 2 *and* the public key of the chip glued to the piece of art
7) Author signature of the file of point 6
8) Signature of the signed file by one or more notaries which biometrically validate the author signature
9) Time stamp application which certifies the data and time of the signatures

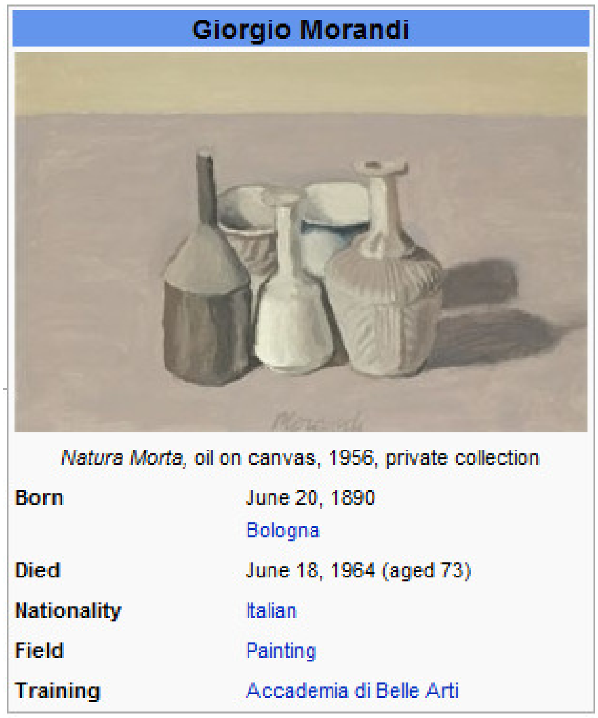


"It is high time for an encounter between art and technology"

Fig. 6

In figure 6 the opening screen of the program is presented. In this example we consider that author data and his digital signature have been already recorded. These two operations can be performed by a "Registration Authority" external to the certification system as it is the case, for instance, in Italy for the Italian digital signature (which is valid for all administrative procedures).

Data regarding the piece of art can be collected off-line and are out of the scope of this context. An example is in figure 7



Giorgio Morandi

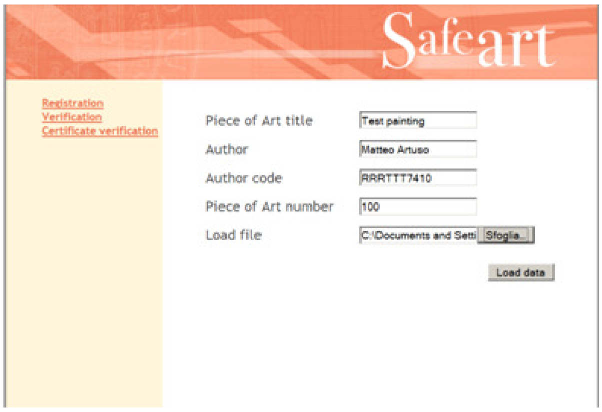
Natura Morta, oil on canvas, 1956, private collection

Born	June 20, 1890 Bologna
Died	June 18, 1964 (aged 73)
Nationality	Italian
Field	Painting
Training	Accademia di Belle Arti

Fig 7

Certifier: Mr X.Y
Date of Certification: aa.bb.cccc
Location of painting:Undisclosed.
………

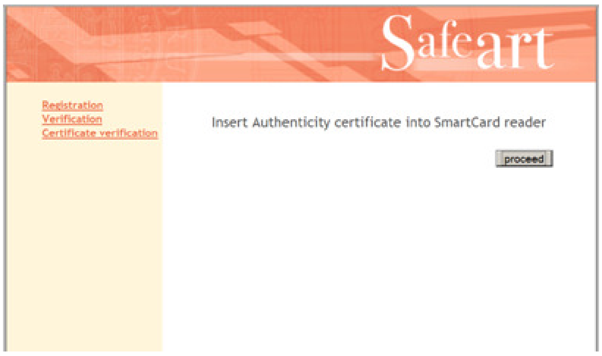
All previous information can be stored for instance in a .PDF file. It is very important to store this information orderly because they must be "human readable" and therefore accessible to the general public.



Piece of Art title: Test painting
Author: Matteo Artuso
Author code: RRRTTT7410
Piece of Art number: 100
Load file: C:\Documents and Setti

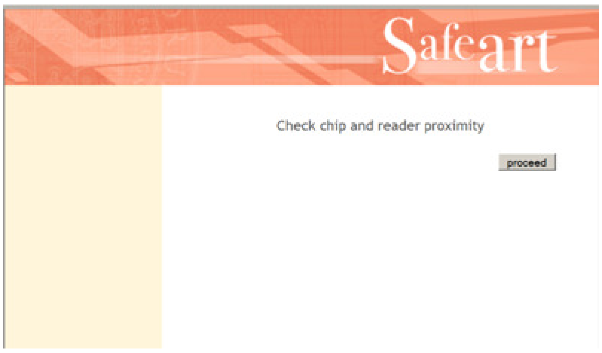
Fig. 8

To the aforesaid document will be linked to the keys pair which will generated by the wireless chip in the following steps. The system through a Java applet can communicate with the reader connected to the client station and therefore with the remote chip and the authenticity certificate. The certifier must only check that the piece of art is close enough to the station and that the smart card of the authenticity certificate is correctly inserted.



Insert Authenticity certificate into SmartCard reader

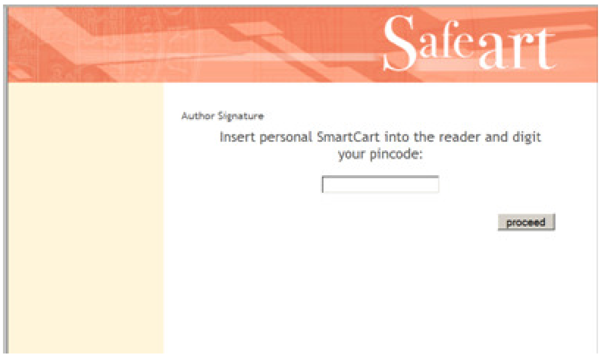
Fig. 9



Check chip and reader proximity

Fig. 10

Both operations are very simple and the system through the java applet will generate the keys pair and will extract the public keys to be associated to the document. Then the certifier through an appropriate command (depressing a key) will activate the procedure. At the end of it the document is complete and the information of point 2 are linked to the public keys of the chip of the piece of art
Then the so produced document with the data and the key pair (*the certificate*) is ready to be signed.

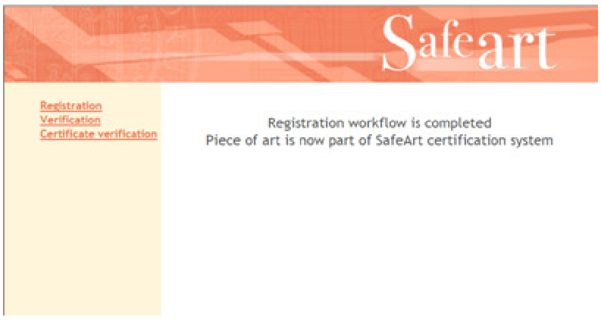


Author Signature

Insert personal SmartCart into the reader and digit your pincode:

Fig. 11

The first signature is that of the author which grants to himself and to the potentials owners the authenticity and the uniqueness of the piece of art. Each piece of art, in fact, has an *unique* certificate and therefore *only a copy* of this piece of art (the authentic one) can exist. Obviously when already existing pieces of art of deceased authors must be certified this step does not take place. The successive signatures are those of the certifiers. In the most normal cases the only signature is that of the responsible of the procedure, a sort of a “notary” of the system but when needed multiple signatures can be added. This is for instance the case of old disputed pieces of art where this procedure replaces the old “expertise” procedure.
All these signatures are independent that is they are added “in parallel” to the document. When all the certifiers have signed the document a certified time stamp is added to the signed document. If all these step where correctly executed the resulting document is stored in the DB and the user will be informed the successful completion of the procedure. From now on the piece of art is censed and its authenticity can be verified (fig. 12)

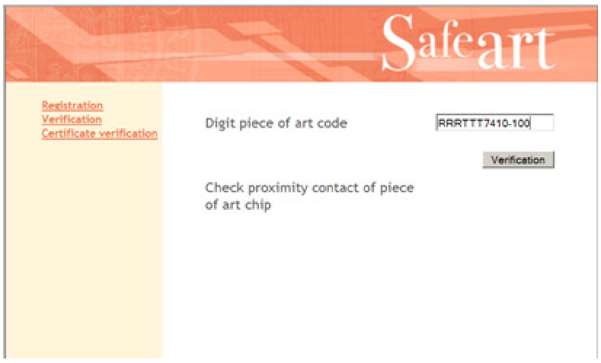


Registration workflow is completed
Piece of art is now part of SafeArt certification system

Fig 12

The connection between the property certificate and the document describing the *piece of art is absolutely safe and can not in any way tampered.*

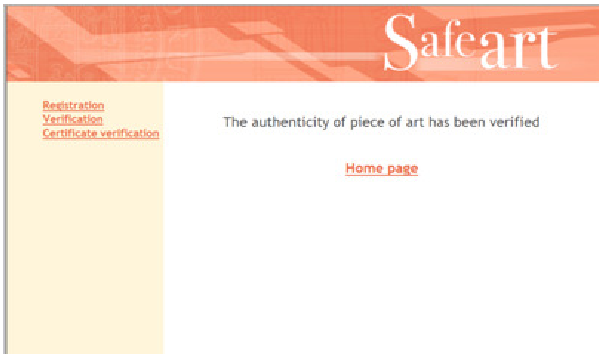
5 – Verification



Digit piece of art code RRRTTT7410-100

Check proximity contact of piece of art chip

Fig. 13



The authenticity of piece of art has been verified

Fig. 14

In figure 13 and 14 the video screens of the verification process is presented which is very similar to the workflow previously presented.

Fig. 15

In figure 15 an hypothetical representation of the use of SafeArt is presented.

6 Security

The authentication heart of SafeArt system is obviously based on the installation of an electronic device, a chip able to implement the aforementioned algorithm for the piece of art to be certified. Before the installation the technological problem of a glue which grants the impossibility of removing the device without damaging the canvas (or any other material) and at the same time protects it against possible glue damage must be tackled and solved. The chip, which is about 2 square millimeters large (but for the antenna) , must become integral part of the piece of art. The impossibility of removal is granted, with the particular glue technology used, for about 15 years, which is the normal life range of an electronic device and the time span beyond which possible improvements of the speed of computers could potentially lead to "crack" by "brute force" the encrypting code (although the problem is n-p complete). It should be remembered that this limit is not intrinsic to this digital signature application field, but is of a general validity. All digital documents MUST be refreshed after a well determined period of time and this applies also to this application. A new device should be put in place of the old one (removable after 15 years) by an authorized body through a legally valid procedure.

The type of glue which has been used protects also the chip against possible electronic tampering. It must be underlined that the small size of the chip (and the related wireless antenna slightly bigger than the chip) allows its use in all possible environments (canvas, marble, plastic etc.): the total size is about a normal jacket button or 20 cents of Euro. It must be underlined that even if the antenna is damaged it is still possible to replace it and the certification process is not impaired (in alternativa harmed o damaged).

The safety of the certification procedure is based also on the particular type of protocol used for communication between the chip and the "base station". The aforementioned ISO 14443, which was developed for the communication of the wireless smart card, is appropriate in this environment both from the electrical and data exchange points of view.

This protocol establishes a “session” between the chip and the remote reader through a “handshake” procedure which grants the integrity of the transmitted data and at the same time prevents possible interference by a third unwanted “party” (reader or chip). The base station is therefore sure that the communication takes place *only* with the particular chip glued to the piece of art with no tampering of the spurious signals which could lead to a false certification or a erroneous rejection of an authentic piece of art. The installed wireless chip, once the communication has been established, can safely communicate *only* with the enabled base station. A diagram of the a protocol is presented in figure 16 while a detailed description can be found in the official ISO document [9].

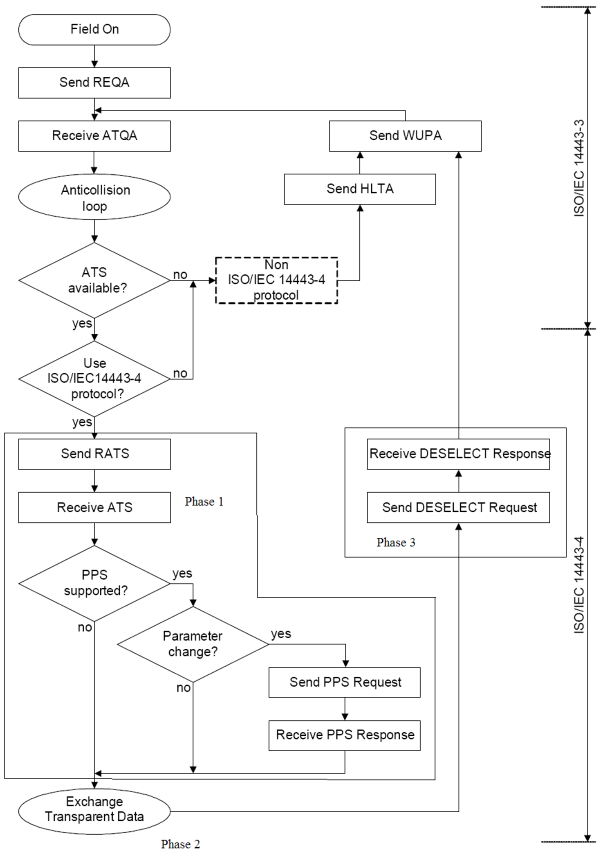


Fig 16

The reader on the registration/verification base station (PCD, Proximity Coupling Device) sends a session initialization command “Request Answer To Select - RATS” to the chip (which is called PICC Proximity Card or Object) which in turn answers with a “Answer To Select ATS” message. The characteristics of the chip are defined on the ATS message: the PCD can send further commands in order to refine the session parameters. The communication parameters are in any case established by the base station: the glued chip can only accept or deny the proposed mode of communication. At the end of the handshake procedure (Phase 1 in the diagram) the real transfer of data between base station and chip takes place.

When a verification procedure is requested, SafeArt through the base station sends a “challenge” message which a request of signature (SIGN) that is the encryption of the received message with the private key of the chip. In the case of registration, the system sends a command requesting the generation of an asymmetric key pair (KEYGEN) followed by a command for retrieving the public key (GETOBIJECT PK).

Each session between PCD reader and PICC chip must finish with a standard sequence that is a DESELECT REQUEST acknowledged by the chip through a DESELECT RESPONSE answer. Although FaseArt is intrinsically safe, since it is based on a public and private key infrastructure, a further important aspect of security id achieved through a PIN code for activating the chip which is stored in the SafeArt database. This is provided for each chip which is installed on a piece of art and it is stored together with the other data, that is the signed file described in the previous paragraphs. This prevents possible attacks to the installed wireless chip both due to its malfunctioning (theoretically possible after several millions of verifications) or its code (RSA 2048 bits) cracking through brute force.

7 SafeArt Scope and Out of Scope

SafeArt grants the existence of a *unique* copy and a registered piece of art. Since a registration protocol is provided the system entrust the responsibility of the initial authentication to the involved users (author, experts, critics of art, authorized certifiers etc.) who upon the registration (time t_0 for the certified piece of art) originate the automatic certification data. SafeArt cannot provide technology for authenticity certification *before* the registration. This type of data (for instance "expertises", identification for ancient paintings) must be otherwise provided and inserted in the certification data.

So far SafeArt does not provide a localization feature although through the installation of a standard wireless protocol chip it can be envisaged its use as a RFID to be used as:

- Monitoring the location of a piece of art in a museum, art gallery etc.
- Detecting, during investigation, possible stolen items which were hidden. These features could be fruitfully exploited by insurances companies, police and so on .
- Electronic guide application. For instance museum visitors could be guided through the exhibition halls and listen to explanations with their headset or PDA without human intervention given their proximity to the pieces of art.

8 SafeArt Catalogue

SafeArt implements a technological link between pieces of art and their digital catalogue in a DB. All information is stored in a Human Readable document (for instance a PDF document) which provides the users with a catalogue which can be safely used with no specific programs and/or infrastructures.

Foundations, museums, institutions which already have a digital archive of their pieces of art can integrate certification data provided by SafeArt in their catalogue and therefore can rapidly (and with small financial costs) activate the service

9 Extensions

The authenticity test is a pervasive problem which affects nowadays almost all fields: just as a matter of example, fashion, food, drugs etc. It is a problem which always involves not only great deal of money (as in the case of fashion where, however, it is highly disputable whether the companies *really* wants a certification system for their *griffes*) but also the health of citizens. As an example in Italy, great producer of high quality hams, we face a great attack from south east Asia whence cheap and low quality hams are smuggled as top quality Italian hams on the ground that the vast majority of the consumers are unable to detect the real difference. The same applies, for instance, to the cheap drugs sold on Internet and so on. Safeart can fight these crimes since it is intrinsically safe but also very inexpensive and it takes only to the fantasy of the potential users to exploit it. And instead of gluing the chip it could be included in a tamper proof cheap case etc. A rough value of the involved costs (PC apart which is almost costless in mass use of the system) the chips (and the case or glue) could be well below one dollar per item ma in millions of items it can fall well below that price. Just consider how much is the cost of a high quality bag of of an entire ham and it is immediately proven the cost-effectiveness of the system. As far as the signature procedure is concerned it can be highly automated so as to be used in a mass production system.

10 Conclusion

A safe, inexpensive and easy to use system has been presented which although originating from the problems of art authenticity can be used in a variety of environments, ranging from fashion to food, drugs etc. The system has been prototyped at Bologna university and is about to be tested in different environments.

References

[1] John Henry Merriman, Counterfeit Art, *International Journal of Cultural Property,* Vol. 1, Issue 01, January 1992, pp. 27-28

[2] New York Times, *ART COUNTERFEIT REVEALED,* 1922, September 24

[3] CNN.COM/crime, *7 indicted in international scheme to sell counterfeit art,* http://www.cnn.com/2008/CRIME/03/19/counterfeit.art/index.html

[4] James M. Hughes, Daniel J. Graham, and Daniel N. Rockmore *Quantification of artistic style through sparse codinganalysis in the drawings of Pieter Bruegel the Elder* Proceedings of the National Academy of Sciences of United States of America published online before print January 5, 2010, doi:10.1073/pnas.0910530107

[5] Rivest R.L., Shamir A., Adleman L. *A method for obtaining digital signatures and public-key cryptosystems,* CACM, 21,2 (Feb. 1978), pp. 120-126

[6] European directive n. 93, December 13th, 1999

[7] Kevin J. Connolly, *Law of internet security and privacy,* Aspen Publishers, 2004, ISBN 0735542732, 9780735542730

[8] ISO 14443, Identification cards — Contactless integrated circuit cards — Proximity cards, http://www.iso.org

[9] ISO 7816, Identification cards — Integrated circuit cards, http://www.iso.org