BAAI: Biometric Authentication and Authorization Infrastructure

Ed Dawson[1], Javier Lopez[2], Jose A. Montenegro[2] and Eiji Okamoto[3]

[1] Information Security Research Centre,
Queensland University of Technology, Australia
e.dawson@qut.edu.au
[2] Computer Science Department, E.T.S. Ingenieria Informatica
Universidad de Malaga, Spain
{ jlm, monte } @lcc.uma.es
[3] Institute of Information Sciences and Electronics,
University of Tsukuba, Japan
okamoto@is.tsukuba.ac.jp

Abstract: The combined use of authorization and authentication infrastructures has led to AAIs (Authorization and Authentication Infrastructures). These new infrastructures supply identification and authorization services to a distributed environment. There are many possibilities of linkages to get AAIs; one of them is to include the PMI (Privilege Management Infrastructure) as Authorization Infrastructure and an Authentication Infrastructure that can be a PKI (Public Key Infrastructure) or Kerberos. This symbiosis gives service to applications and servers. However, in physical environments where the physical presence of an individual is required, it is necessary to use biometric systems. This paper describes the development of a solution that combines the relationship between the biometric based systems and the PMIs to finally obtain the Biometric AAI.

Keywords: AAI, Attribute Certificate, Authentication, Authorization, Biometric, Identity Certificate, PKI, PMI, Steganography.

1. Introduction

Applications increase the use of Internet as a communication media. This situation has made it necessary to export the authorization and authentication mechanism from centralized systems to distributed systems.

X509 *identity certificate* [ITU97] made feasible distributed authentication based on a link between a public key and the proprietor's name. This link is testified with the signature of a trusted authority.

There are applications that need authorization services in addition to authentication services. The new approach of certificate, X509 *attribute certificate* [ITU00], binds a user to his/her attributes, role assignation and privilege delegation of other entities.

The possibility of binding the attribute certificate and the identity certificate establishes in an easy and natural manner an Authorization and Authentication Infrastructure (AAI). The AAIs endow services to applications to identify that need a determinate service and what is possible to do with this service. The work [Daw02] details the possible bind between a PMI and an external organization PKI (*outsourcing PKI*). The reason is that the authentication can be contributed to public organization, because it has legal and intrinsic character, whereas the authorization has a more private character and normally need to be administrated to an entity that has a relation with the organization. Another possibility is to bind the PMI with Kerberos system. This option changes an identity certificate to Kerberos tickets. These binds let a user access into the system and subsequently the system to authorize him to do determinate tasks. This scheme makes possible the delegation between the servers and it is possible to make a trust path to access to a resource independently where it is located.

In certain situations the physical presence of the individual for its identification is necessary. This is achieved by using physical characteristics for recognition in a biometric system. A biometric system can be also take part in an AAI by a correct bind to a PMI. This work is about a possible solution to bind both technologies, Biometrics and PMI, to obtain a *BAAI* (*Biometric Authentication and Authorization Infrastructure*), using steganography that optimises and facilitates the union.

This paper presents PMI, Steganographic techniques and Biometric techniques in sections 2, 3, and 4, respectively, as the building technologies used in our BAAI scheme, which is presented in section 5. Finally, section 6 contains conclusions.

2. First Building Block: The PMI

ITU-T Recommendation X.509 of year 2000 has defined PMI as the framework for the wide use of attribute certificates. The Recommendation includes the data object specification to represent this type of certificate, that is, it defines the attribute certificate structure, which is similar to its predecessor, the identity certificate. This similarity can be seen in not only in the mandatory certificate fields: *version*, *serial number*, *signature algorithm*, *issuer*, and *validity period*, but also in the optional fields: *issuer unique identifier* and *extensions*. There are two fields in the attribute certificate structure that are new regarding the identity certificate. These are the fields *holder*, that conveys the identity of the attribute certificate's holder, and *attribute*, that contains the attributes associated with the holder that are being certified (e.g. the privileges).

Similarly to identity certificate, there is a trusted third party entitled to sign attribute certificates. In this case the third party is called *Attribute Authority* (AA), who assigns privileges. The privilege assignment has a top-down basis. The root of the hierarchy is the *Source of Authority* (SOA), the entity that is trusted by a privilege verifier as the entity with ultimate responsibility for assignment of a set of privileges. Also similarly to PKIs, the PMI inherits the concept of revocation lists. This is called *Attribute Certificate Revocation Lists* (ACRL), which essentially have the same format and management structure as the typical CRL. All of these elements together constitute the Privilege Management Infrastructure.

Although the recommendation is recent, there are already some practical initiatives. Probably, the most representative is *PERMIS* (Privilege and Role Management Infrastructure Standards validation), a research European Project of the Fifth Framework Programme. This project relies on the ITU standard, and it is an excellent practical reference to show the use of attribute certificates in applications that require access control [Cha02].

Other interesting initiatives related to Authorization services, although not following ITU standards, are the *Akenti* system [Tho03], developed at Berkeley, the *PAPI* system [Lop02], developed by the Spanish National Research Academy, and the *AAARCH Architecture* [Gom02], designed in the scope of the Internet Research Task Force.

3. Second Building Block: Steganography Techniques

Steganography is the art of hiding and transmitting data through apparently innocuous carries in an effort to conceal the existence of the data. The word steganography, as derived from Greek, literally means covered or hidden writing and includes a vast array of methods of secure communications that conceal the existence of the message. Computer-based stenographic techniques introduce changes to digital covers to embed information foreign to the native covers (figure 1).

Steganography encompasses methods of transmitting secret messages in such a manner that the existence of the embedded messages is undetectable. Carriers of such messages may resemble innocent sounding text, disks and storage devices, network traffic and protocols, audio, images, video or any other digitally represented code or transmission [Joh01].

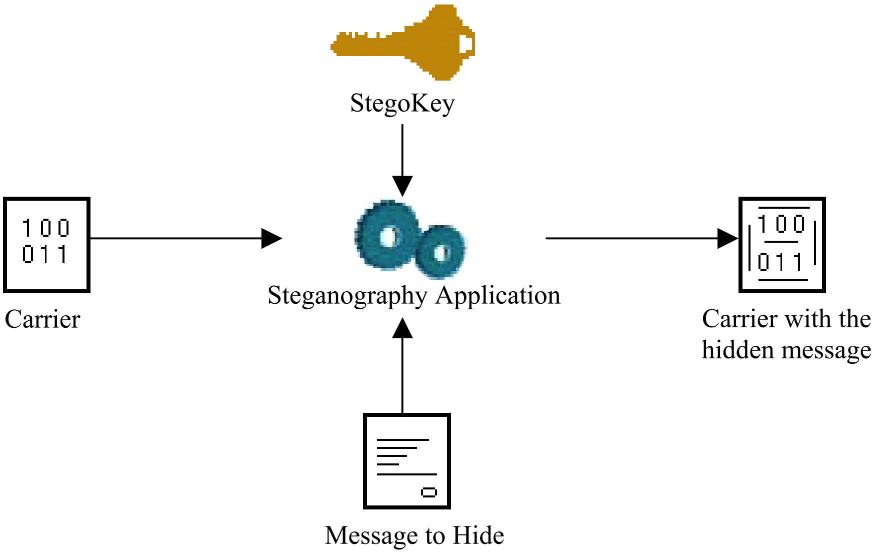


Figure 1. Steganography: General Scheme

Normally the attack against hidden information is performed when it is detected inside the carrier. However, it is possible to perform distortion or removal attack without knowing the message enclosed, but destroying its content.

In our approach, the detection of attack against the information is not a critical issue because, as we will show later, we embed a message into the figure without hiding purposes. In fact, the information to embed is public. This means that in our design we make use of steganography techniques just to send an object O_1 inside another object O_2, and to bind those data structures, but not to hide O_1. The situation is not the same for data distortion or removal attacks. In this case, a denegation of service is produced because it will be impossible to get part of the information needed.

3.1 Steganography using Digital Images

Digital image is an array of numbers that represent light intensities at various points (pixels). Theses pixels make up the visible information. A common image size is 640 x 480, and such an image could contain about 300000 pixels. Pixels are typically stored as either 24-bit or 8-bit.

The method used to hide the information in the images is *least signification bit* (LSB) insertion or manipulation. This method does not produce a change in the pixel intensity as to be detected by the human eye. The resulting stego-image will look identical to the cover image.

To hide information in the LSBs of each byte of a 24-bit image, one can store three bits in each pixel. A 1024 x 768 image has the potential to hide 294,912 bytes of information. For example, as shown, the letter ‘A’ (10000011) can be hidden in three pixels. The left matrix is the original information while the right matrix shows, in bold font, the bit changes that are necessary to hide the information.

(00100111 11101001 11001000)	(00100111 1110100**0** 11001000)
(00100111 11001000 11101001)	(0010011**0** 1100100**0** 1110100**0**)
(11001001 00100111 11101001)	(11001001 00100111 11101001)
Original Data	**Altered Data to hide letter ‘A’**

3.2 Steganography Tools to work with Digital Images

Steganographic tools are introduced in [Way02] [Joh01] that make possible the easy use of this technology. Most of the tools are freeware or shareware, and it is possible to use the source code of steganographic algorithms. The use of source code could be an advantage to make a routine library that facilitates the integration with other technologies used in our approach.

The application of steganographic techniques to digital images depends on image quality and on the codification to store the image. Therefore, there are different steganography applications that support different image formats. For instance, the application used in our system is *S-Tools* (Stenography Tools) that support GIF and BMP graphic formats. In case of using an image in JPEG format, we use either the *Jsteg* algorithm or one of its successors, *F4* and *F5* that solve statistical deficiencies of the former.

This situation may limit versatility of our approach, which can be easily solved by implementing a routine library that makes the approach independent from the graphic format.

4. Third Building Block: Biometric Techniques

The ever increasing human population and its mobility in all its facets has caused security in organizations to become an important social issue. As mobility applies to both humans and information, security includes both security of individuals and their valuables, and the integrity of data under external influence.

Within this scenario, development of identification and authentication techniques is essential, and among these techniques, biometric ones are outstanding. Operation of biometric devices can be explained with the following three-step procedure:

1. A sensor takes an observation. The type of sensor and its observation depend on the type of biometrics device used. This observation provides us with a *biometric signature* of the individual.

2. A computer algorithm normalizes the biometric signature and produces information with a determined format (size, resolution, view, etc). This format will allow a later comparison with the information stored in the system's database of the identity verifier. Such a normalization process provides a *normalized signature* of the individual.

3. A matcher, part of the identity verifier, compares the normalized signature whit the set (or subset) of normalized signatures on the system's database and provides a *similarity score*.

Generally speaking, there are two kinds of biometric systems: *identification* and *verification* systems [Phi00]. When using identification ones, a biometric signature of an unknown person is presented to a system. This compares the new biometric signature with the database of biometric signatures of the known individuals. Based on the comparison, the system reports or estimates the identity of the unknown person from this database.

When using verification systems, a user presents a biometric signature and a claim that a particular identity belongs to the biometric signature. The algorithm either accepts or rejects the claim. Alternatively, the algorithm can return a confidence measurement of the claim's validity.

Figure 2 [Mans02] establishes the basic components of a general biometric system, and details the communication between the components and the communicated data.

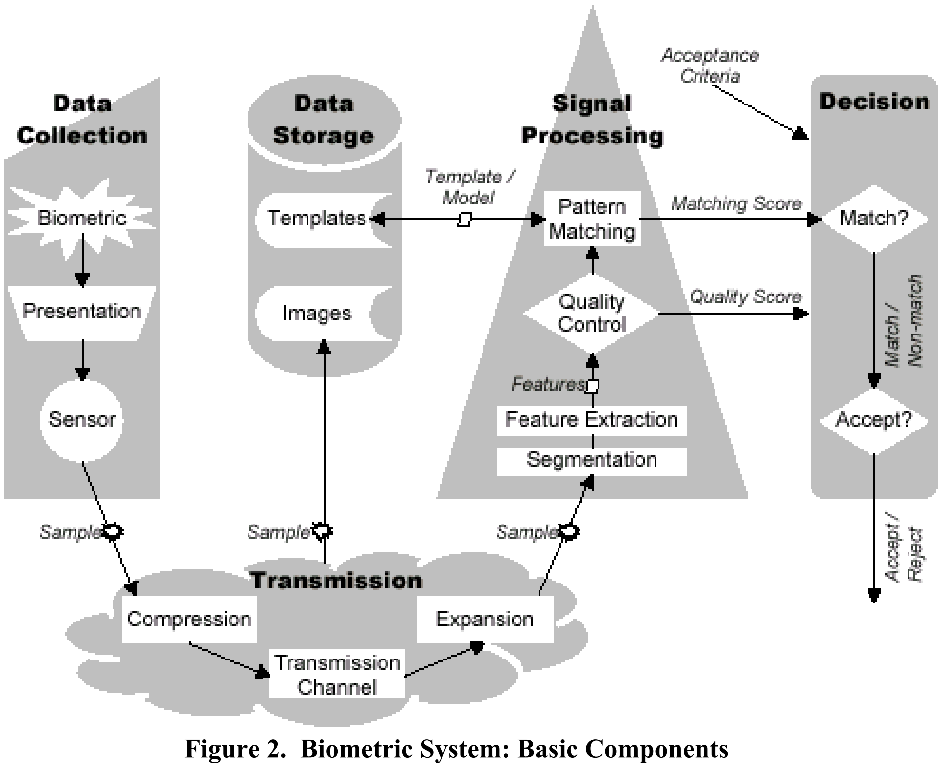


Figure 2. Biometric System: Basic Components

In the following we explain figure 2, left to right direction, that is, from data acquisition process to decision on the acceptance or rejection. In the sequence, the biometric data (*sample*) is captured by a sensor, compressed, sent using any transmission media, and finally uncompressed in the receiver. A mathematical representation (features) of the information extracted from the presented sample will be used to compare with enrolment templates, in order to take a final decision (accept or reject).

An ideal biometric system would have the following features:

- all members of the population possess the characteristic that the biometric identifies, like irises or fingerprint;
- each biometric signature differs from all others in the controlled population;
- the biometric signatures do not vary under the conditions in which they are collected; and
- the system resists countermeasures.

Individuals possess different features that allow the use of diverse biometric systems, such as face, voice and fingerprint recognition. Our approach is based on face recognition, but the methods we have used are easy to extrapolate to other biometric techniques.

4.1 Face Recognition

In the 1990s, automatic face recognition technology moved from the laboratory to the commercial world because of the rapid development of the technology [Wec98].

Broadly speaking, the necessary steps for the correct operation of the face recognition are location of eyes inside the head, and location of the head itself inside the picture. Then, a matrix based on the characteristic of the individual face is generated. The method of defining the matrix varies according to the algorithm used. This matrix is then compared to matrices that are stored in a database, and a similarity score is generated for each comparison.

In order to organize the vast field of face recognition the work of Fromherz et al.[Fro97] presents a high and low level classification of possible solutions to face recognition. The high level classification distinguishes between frontal and profile recognition. On the other hand, low-level classification aims at immediate problems in face recognition. For instance, algorithms treating the face and its environment as uncontrolled systems can be differentiated from systems where lighting or background of the scene, as well as orientation of the face, are under control. The type of control that uses one or more images for the recognition task can also be differentiated from others that are based on video sequences.

The work by Zhao et al. [Zha00] details a list of face recognition applications, as biometric, information security, smart cards, law enforcement and surveillance and access control. That paper surveys the state of the art in face recognition and the possible inconveniences present in the technology.

4.2 Face Recognition Tools

FERET (Face Recognition Technology) Project provides the most useful technical information about face recognition [Phi96]. FERET is sponsored by the Department of Defense Counterdrug Technology Development Program through the Defense Advanced Research Projects Agency (DARPA), with the U.S. Army Research Laboratory (ARL) serving as technical agent.

The project has three major tasks. The first one is the development of the basic technology required for a face recognition system. The second task is the collection of a large database of facial images. This database has been essential for the later development of this technology since the information is available as standard information with which to compare the algorithms developed by the scientific community. The third task is government-monitored testing and evaluation of face recognition algorithms using standardized test procedures.

The purpose of the tests has been to measure overall progress in face recognition, determine the maturity of face recognition algorithms, and have an independent mean of comparing algorithms. The tests measure the ability of the algorithms to handle large databases, changes in people's appearance over time, variations in illumination, scale, and pose, and changes in the background.

Upon finalization of FERET Project in 1997, more outstanding information for the evaluation of the face recognition technology was published [Phi98][Riz98]. This evaluation was extrapolated to commercial products in the market until year 2000 [Bon01]. Interest in face recognition has increased after terrorist attacks on September 11th, and many government agencies have been considering the use of face recognition systems in airports and other important locations in order to search for known terrorists or to control access to secure areas. This situation has entailed to the publication of a recent report of evaluation of the technology [Bon02].

In addition to the information provided by project FERET, it is possible to find applications that implement the algorithms of face recognition. We have used the results of a research project at Colorado State University about a "Face Identification Evaluation System" [Bol03]. The results provide three standard face recognition algorithms and standard statistical methods to evaluate the algorithms and standardized image pre-processing software.

5. Our Scheme: Biometric AAI (BAAI)

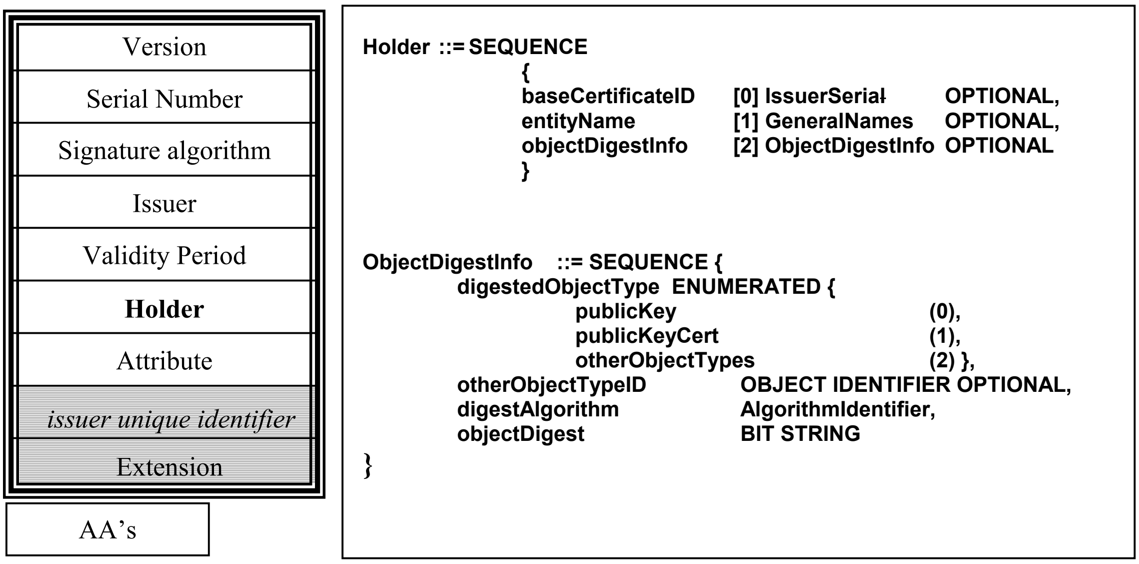
As mentioned, biometric techniques allow us to conduct operations of identification and authentication in systems that require human presence. This eliminates the need of storage of secrets shared between system and user, since it uses intrinsic characteristics of the humans for such task.

Once the user has authenticated to the system, it is necessary to know which tasks are granted for. Therefore, it is necessary to specify the privileges that the individual in the system have been assigned.

The work presented in [Kon96] uses a biometric system based on genetic algorithms. This system associates privileges to existing images of the user by means of a graphical interface. This approach to the problem addressed here becomes unsatisfactory when we transfer the allocation of privileges from a centralized system to a set of distributed resources. In the distributed case it is more suitable to use a PMI.

5.1 Technical Description of Approach

The field *Holder* in the X509 attribute certificate represents the identity of the user, the privileges possessor. As is shown in figure 3 (codified in ASN1 [ASN1]), such field can be composed by a sequence of items, enabling to tie the privilege with: (i) the user's identity certificate, (ii) an identifier, or (iii) the digest of an object.



```
Holder ::= SEQUENCE
                {
                baseCertificateID    [0] IssuerSerial        OPTIONAL,
                entityName           [1] GeneralNames        OPTIONAL,
                objectDigestInfo     [2] ObjectDigestInfo    OPTIONAL
                }


ObjectDigestInfo    ::= SEQUENCE {
        digestedObjectType  ENUMERATED {
                    publicKey                           (0),
                    publicKeyCert                       (1),
                    otherObjectTypes                    (2) },
        otherObjectTypeID           OBJECT IDENTIFIER OPTIONAL,
        digestAlgorithm             AlgorithmIdentifier,
        objectDigest                BIT STRING
}
```

Figure 3. Binding Attributes to the identity

Our approach uses the two last fields of the eventual sequence for *Holder*, following this process:

1. We obtain an image of the user's face and perform a hash function of its most significant bits.

2. The hash of the image is stored in the *ObjectDigestInfo* field, while the field *entityName* contains the user's name. This mechanism allows the Authorization Authority to simultaneously have the role of a Certification Authority. Thus, we get an AAIs with a single infrastructure, eliminating the cost of a separate PKI and PMI management. It is important to note that in our solution this is achieved without changing what the standard proposes.

3. The AA performs all those tasks related to authorization, introducing in the certificate the attributes or allocation of roles of the identified user.

4. Once the binding between the user's image and his/her attributes is completed, the certificate is introduced inside the image by using steganographic techniques. This allows having a single object with all the authentication and

authorization information that is required. The use of steganography will allow that an attribute certificate does not interfere in the recognition of the image by the biometric device. We call the new structure *Visual Attribute Certificate* (VAC).

Figure 4 shows the system operation. Part *a* depicts the certificate creation process where (i) the user identity is bound with his face image for biometric identification, and (ii) the Attribute Authority assigns the privileges by introducing the attributes in the certificate. Part *b* shows how the certificate is introduced in the user's face image by means of a steganographic application.

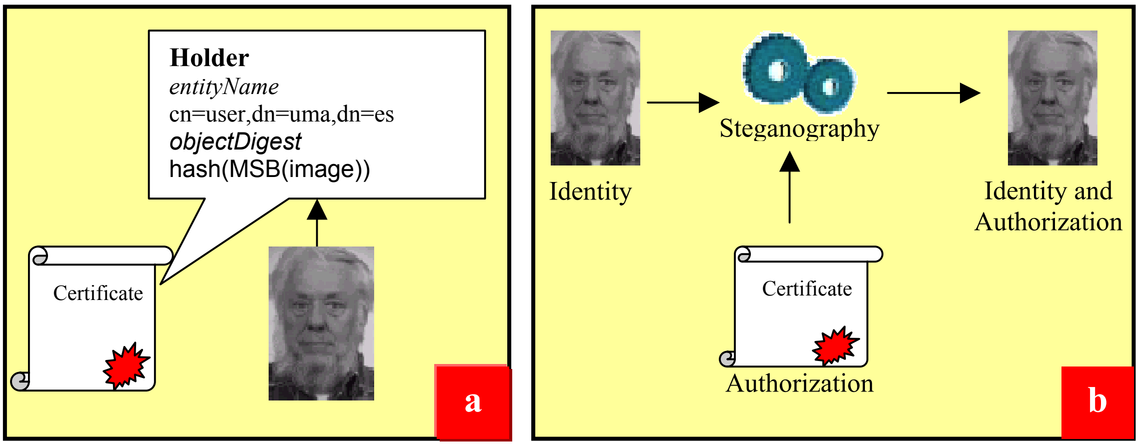


Figure 4. VAC Creation Process

We must point out that step 1 did not use the least significant bits of the image. The reason is that those bits are not used because of the later inclusion of the certificate inside the user's face image would delete them, as explained in section 3.1. Obviously, these bits will not be used later in the verification process.

Once detailed the system operation, we specify the authentication and authorization process, depicted in figure 5. A global overview is shown in figure 6.

1'. The camera obtains the face image of the user.

2'. The system compares that image with the VAC (identification process)

3'. If the user is correctly identified, the system extracts the attribute certificate and the privileges of the user previously identified are accessed.

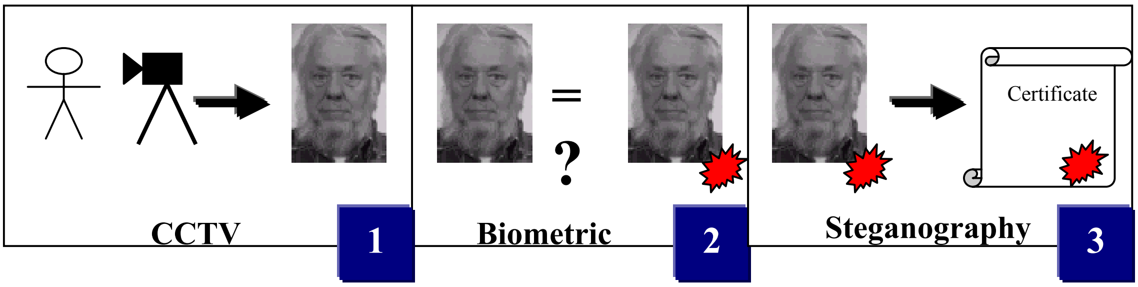


Figure 5. Authentication and Authorization Process

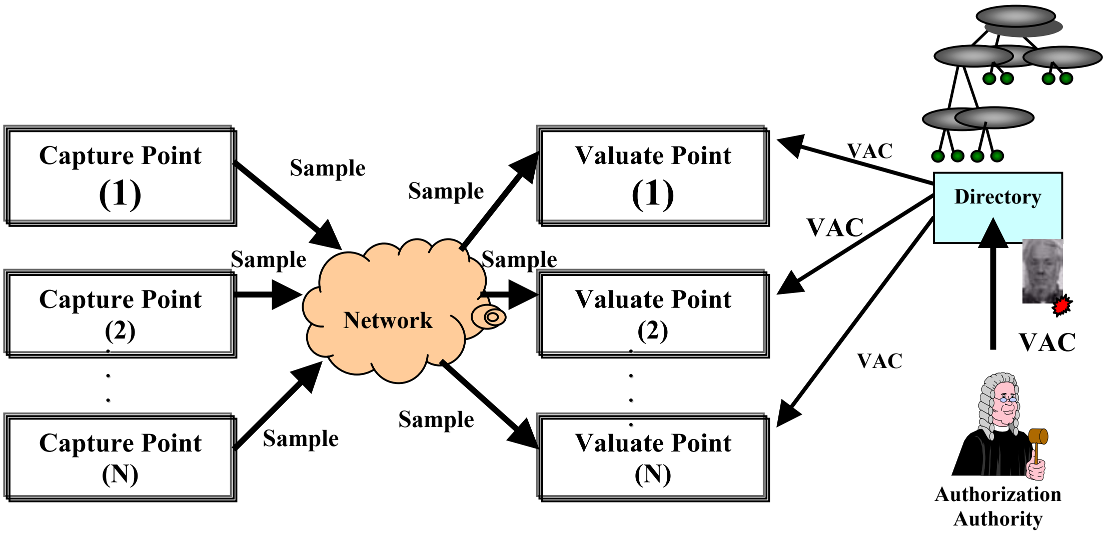


Figure 6. Global Overview

6. Conclusions and Future Work

AAIs combine authorization and authentication capabilities for distributed environments. There are several possibilities of linkages to get AAIs. One of them is to use a PMI as an Authorization Infrastructure and a PKI as an Authentication Infrastructure.

However, in certain situations the physical presence of the individual is necessary for its identification. In these cases, it is convenient that a biometric system takes part in the AAI too. The present work has presented a possible solution to bind biometrics and PMI technologies. We have designed what we have called a BAAI, what stands for “Biometric Authentication and Authorization Infrastructure”, and its design has been influenced by the use of steganographic techniques, which optimise and facilitate the merge.

Precisely, by using steganography, we have created a new type of object, the Visual Attribute Certificate, that allows having all authentication and authorization information in a single object.

References

[ASN1] Kaliski ”A Layman’s Guide to a Subset of ASN.1, BER, and DER”, November 1993

[Bol03] Bolme, David; Teixeira, Marcio; Beveridge, J.Roos; Draper, Bruce; “The CSU Face Identification Evaluation System: Its Purpose, Features and Structure”. International Conference on Computer Vision Systems 2003

[Bon01] Bone, Mike; Blackburn, Duane, Phillips; “Face Recognition Vendor Test 2000 Evaluation Report”. February 2001

[Bon02] Bone, Mike; Blackburn, Duane; “Face Recognition at a Chokepoint. Scenario Evaluation Results”. November 2002

[Cha02] Chadwick,D.; Otenko, A.; “The PERMIS X.509 Role Based Privilege Management Infrastructure”. Future Generation Computer Systems, 936 (2002) 1–13, December 2002.

[Daw02] Dawson, E.; Lopez, J.; Montenegro, J.A.; Okamoto, E.; “A New Design of Privilege Management Infrastructure for Organizations Using Outsourced PKI”, 5th Information Security Conference, ISC 2002, Sao Paulo, Brazil (2002) 136-149.

[Fro97] Fromherz, T.; Stucki, P.; Bichsel, M. “A survey of face recognition”, MML Tech. Rep. 97.01, Dept. Comp. Sci., Univ. of Zurich, 1997.

[Gom02] Leon Gommans, Cees de Laat, Bas van Oudenaarde, Arie Taal, "Authorization of a QoS Path based on Generic AAA", A special issue of FGCS on the iGRID2002 conference, Amsterdam, September 2002.

[ITU97] ITU-T Recommendation X.509, ”Information Technology - Open systems inter-connection- The Directory: Authentication Framework”, June 1997

[ITU00] ITU-T Recommendation X.509, ”Information Technology - Open systems interconnection- The Directory: Public-key and attribute certificate frameworks”, 2000

[Joh01] Johson, Neil; Duric, Zoran; Jajodia, Sushil ; “Information Hiding: Steganography and Watermarking – Attacks and Countermeasures”. Kluwer 2001

[Kon96] Konen, Wolfang; Schule-Krüger, Ekkerhard; “ZN-Face: A system for access control using automated face recognition”, Neural Networks: Artificial Intelligence and Industrial Applications. Proceedings of the third annual SNN Symposium on Neural Networks, Nijmegen, The Nertherlands, 1995.

[Lop02] Lopez, D.R.; Castro, R; ”Ubiquitous Internet Access Control: The PAPI System”. International Workshop on Trust and Privacy in Digital Business - TrustBus 2002. September 2002.

[Man02] Mansfield, A.J.; Wayman, J.L.; “Best Practices in Testing and Reporting Perfomance of Biometric Devices” Technical Report, Centre of Mathematics and Scientific Computing, NPL Report CMSC 14/02 , August, 2002.

[Phi96] Philps, P. Jonathon; Rauss, Patrick J.; Der, Sandor Z.; “FERET (Face Recognition Technology). Recognition Algorithm Development and Test Results”. Technical Report ARL-TR-995. 1996

[Phi98] Phillips, P. Jonathon; Moon, H. M.; Rizvi, S.A.; Rauss, P.J.; “The FERET Evaluation Methology for Face Recognition Algorithms” NISTIR 6264, National Institute of Standard and Technology, 1998

[Phi00] Phillips, P. Jonathon; Martin, Alvin; Wilson, C.L.; Przybocki, Mark; “An Introduction to Evaluating Biometric Systems” IEEE 2000.

[Riz98] Rizvi, S.A.; Phillips, P. J.; Moon, H. M.; “The FERET Verification Testing Protocol for Face Recognition Algorithms” NISTIR 6281, National Institute of Standard and Technology, 1998

[Tho03] Thompson, M.; Essiari, A.; Mudumbai, S.; “Certificate-based Authorization Policy in a PKI Environment” Submitted to a special issue of ACM Transactions on Infomation and System Security, Aug 2003.

[Way02] Wayner, Peter. “Disappearing Cryptography. Information Hiding: Steganography and Watermarking” Morgan Kaufmann 2002.

[Wec98] Wechsler, H. et al., “Face Recognition: From Theory to Applications”, Springer-Verlag, Berlin, 1998.

[Zha00] Zhao, W. Y.; Chellappa, R.; Rosenfeld, A.; Phillips, P. J.; “Face Recognition: A Literature Survey”, UMD CfAR Technical Report CAR-TR-94 8, 2000.