Electronic Signature and Digital Identity
Guest Editors: Javier López-Muñoz, Apol·línia Martínez-Nadal, and Ahmed Patel

Joint monograph with NOVÁTICA*

From the Editors’ Desk
New Developments in UPGRADE and UPENET
The Editorial Team of UPGRADE announces that Mondo Digitale, digital journal published by the Italian CEPIS society AICA, has joined UPENET and that two persons have joined the Editorial Team.

Electronic Signature and Digital Identity

3 Presentation
Electronic Signature as the Key to Security in the Information Society – Javier López-Muñoz, Apol·línia Martínez-Nadal, and Ahmed Patel

The guests introduce the monograph and present the papers included in it, that cover some technical and legal aspects of Electronic Signatures, a key concept for the development of many important application areas such as e-Government or e-Commerce.

6 Electronic Signature at the Heart of Information Security Development: An Overview – Arturo Ribagorda-Garnacho

The authors explain the concept of digital signature and justify the need for public key certificates.

11 Creating a Cross-Domain Public Key Infrastructure: The Keystone Project – Ahmed Patel

A scalable and robust architecture for the cross-domain Public Key Infrastructure (PKI) is described in this paper.


In this paper the authors take a close look at certification practices as statements as vital component of a proper framework for the use of electronic signature, and comments on the experience of the Spanish National Mint.

18 Electronic Signature Functionality and Security Requirements – Gemma Dèler-Castro and Juan-Carlos Cruellas-Ibarz

The authors analyse the value of electronic signature as a symbol of assurance and trust in the virtual world.

23 Electronic Signature Today: A Manufacturer’s Viewpoint – Francisco Jordán-Fernández and Jordi Bach i Tarrats

The authors present the vision that their company, Safelayer, has of the current situation of PKI and electronic signature technologies.

28 Development of an Integrated Document Management System with Advanced Electronic Signature Service – Iñaki Echevarría-Larrinaga, Oscar García-Jimeno, Juan-Antonio Martín-Zubiaga, Víctor Llorente-Gómez, and Javier Areitio-Bertolín

In this paper the design, architecture, functionalities and technologies used in the development of a scalable, distributed and fault tolerant system integrating document management within a public key infrastructure are described.

35 Digital Signatures and Electronic Documents: A Cautionary Tale Revisited – Petr Švéda and Václav Matyáš Jr.

The authors identify and analyse different types of trust and provide a broad overview of how they affect the use of digitally signed documents.

39 Electronic Signature: An Analysis of the Main European and International Legal Regulations – Nadina Foggetti

This paper compares the United Nations Model Law with the European Directive and describes the various ways that the latter has been implemented in several European countries.

47 Electronic Signatures and Electronic Identity Card in the European Context and in Spanish Law – Apol·línia Martínez-Nadal

The author comments on the Spanish Law on electronic signature within the framework of the European legislation as well as what is known as electronic ID.

51 The UNCITRAL Model Law on Electronic Signatures – Rafael Illescas-Ortiz

This paper describes the 2001 United Nations Model Law on electronic signatures and how it has been adopted internationally.

55 Legal Initiatives on Electronic Signature in Latin America – Mariliana Rico-Carrillo

The author takes a look at the content of regulatory laws on electronic signature that are in place in several Latin American countries.

60 The Bilingual Voice Portal in the Arab Region: Voice Browsing in Arabic, English, or Mixed Language – Habib Talhami

This paper presents an approach to building a bilingual (Arabic/English) voice portal by exploiting existing standards such as VoiceXML (eXtensible Markup Language).

65 Asin: New Applications for New Users’ Information Environments
(Three Questions to Prof. Moira Norrie, ETH Zurich, Switzerland)

by François Louis Nicolet

Next issue (August 2004): “Software Agents”
(The full schedule of UPGRADE is available at our website)

Mosaic

67 From “Mondo Digitale” (Italy):
Personal Identification Systems – Furio Cascetta and Marco De Luccia

This article describes the main techniques used for the automatic identification of people in today’s societies.

* This monograph will be also published in Spanish (full issue printed; summary, abstracts and some articles online) by NOVÁTICA, journal of the Spanish CEPIS society ATI (Asociación de Técnicos de Informática) at <http://www.ati.es/novatica>. And in Italian (online edition only, containing summary abstracts and some articles) by the Italian CEPIS society ALCI and the Italian IT portal Tecnoteca at <http://www.tecnoteca.it>.

UPENET (UPGRADE European NETwork)

67 From “Mondo Digitale” (Italy):

Personal Identification Systems – Furio Cascetta and Marco De Luccia

This article describes the main techniques used for the automatic identification of people in today’s societies.

* This monograph will be also published in Spanish (full issue printed; summary, abstracts and some articles online) by NOVÁTICA, journal of the Spanish CEPIS society ATI (Asociación de Técnicos de Informática) at <http://www.ati.es/novatica>, and in Italian (online edition only, containing summary abstracts and some articles) by the Italian CEPIS society ALCI and the Italian IT portal Tecnoteca at <http://www.tecnoteca.it>.
Personal Identification Systems

Furio Cascetta and Marco De Luccia

This article describes the main techniques used for the automatic identification of people. The main characteristics, advantages and limits of each method (fingerprint, iris and retina recognition, voice recognition, etc) are outlined. The typical application fields for each type of personal identification system are reported highlighting their possible future developments.

Keywords: Automatic Identification, Biometrics, Face Recognition, Feature Extraction, Fingerprint Recognition, Hand Recognition, Iris Recognition, Personal Identification (PI), Signature Recognition, Voice Recognition.

1 Definitions and Classification

As a starting point, it is important to introduce certain basic definitions and to classify the different AIDC (Automatic Identification and Data Capture) technologies, highlighting their functions and specific features. As shown in Figure 1, there is a variety of AIDC technologies available today which can be classified in two broad categories:

a. Data Carriers: this category includes the technologies aimed at the “capture, storage and transfer” of data and information mostly encoded on adequate devices. Optic methods (mainly barcodes), techniques based on magnetic storage (magnetic band) and those based on electronic storage (RFID – Radio Frequency Identification – tag, smart card, chip, smart label, etc.) are all part of this category.

b. Feature Extraction: this category comprises three sub-groups according to the type of feature ‘extracted’, i.e. the image of an object or person (vision system), the dynamic characteristic of a person (voice, signature, gait, etc), or a characteristic connected to a chemical-physical property of the material of an object (for example the complex chemical compounds responsible for smells and odors.)

This article will deal with the main technologies used for the identification of people based on biometric recognition (Figure 2) and in particular:

• personal identification based on the biometric recognition of “static features”: capture and processing of human images (anatomic characteristics) such as fingerprints and vascular hand ‘prints’, facial, iris and retinal geometry;

• personal identification based on the recognition of “dynamic features”: vocal timbre, speech peculiarities (spectral analysis of the sound field), dynamic signature (pressure), digitization (pressure), gait (steps in walking.)

2 Biometric Identification Systems

These ‘intelligent’ recognition techniques entail the use of expert systems, neural networks, fuzzy logic systems and the development of sophisticated computing. The main advantages of these methods over traditional ones are connected to their ability to remember and learn.

For a long time, scientists have aspired to the creation of machines and systems capable of imitating certain human abilities, among which the identification based on biometric recognition or the identification through the acquisition and subsequent processing of images.

The main areas of interest of biometric technologies are:
• direct authentication and verification of personal identity (proof of the identity stated by the individual);
• indirect identification of a person through the available biometric characteristics.

The main physiologic or behavioural characteristics that may be used for personal identification must meet the following essential requirements (Figure 3):
• universality (each individual must have the characteristics that have been defined);
• uniqueness (it is not possible for two people to be the same in terms of the characteristics);
• permanence (biometric characteristic must remain unchanged in time);
• collectability (in the sense that biometric characteristic can be measured quantitatively.)

So, the word “biometrics” is used to refer to the study of the automatic methods of identification or authorization of people which entail the use of physiologic and behavioural characteristics. Examples of biometric techniques are: recognition of hand geometry, fingerprints, iris images, facial images, speech, and signature.

Satisfactory results may be obtained by combining two or more recognition techniques.

There are also other recognition techniques among which retina image comparison, voice matching, DNA matching but they are not widely employed due to their complexity. A more general classification of biometric recognition has to do with static aspects (i.e. fingerprints, geometry of the hand, face, iris, etc.) and dynamic aspects (i.e. voice, signature, gait, etc.)

2.1 Personal Identification Based on Biometric Recognition of “Static Aspects”

The main “intelligent” methods of biometric recognition through static aspects are:

a. fingerprint recognition;

b. face recognition;

c. iris and retina recognition;

d. hand recognition.

2.1.1 Fingerprint Recognition

Fingerprint recognition has been used for over a hundred years and is the oldest person-
Biometric recognition techniques were developed by F. Galton and E. Henry around the end of the 19th century. A fingerprint consists of a series of composite segments. It was Galton who demonstrated the uniqueness and permanence of fingerprints. Henry’s studies, on the other hand, led to the creation of a first model of the global structure of a fingerprint (the famous “Henry system” for the classification of fingerprints).

At the beginning of the 20th century fingerprints were already accepted as a valid means of personal identification. Obviously the manual identification through fingerprints was a long, tedious and expensive procedure. So, in 1960 the London and Paris Police started to make the first attempts to create an automatic system of fingerprint identification. More recently, the pioneering work of Galton and Henry was further developed and perfected.

There are two particular ‘aspects’ which characterize a fingerprint: the so called core points and delta points (Figure 4).

The block diagram of an Automatic Fingerprint Authentication System (AFAS) is represented in Figure 5. The input to the AFAS system is the image of the fingerprint and the identity of the corresponding individual; the output is a Yes/No answer. The AFAS system compares the input image with a reference image stored in the identity archive (database).

On the other hand, in an Automatic Fingerprint Identification System (AFIS), as shown in Figure 6, the input consists only of a fingerprint and the output is a list of identities of people whose fingerprint images are stored in the database with a ‘score’ for each identity which indicates the degree of resemblance with the input fingerprint.

The oldest and best known method for ‘capturing’ fingerprint images is by coating the subject’s fingertips with ink and to proceed as if the finger were an ordinary ink pad stamp. The image thus obtained may be distorted and therefore not reliable.

Better results may be obtained with digital systems such as image acquisition through a micro camera which scans the fingerprint. Even in this case distorted images might be obtained due to skin dryness, perspiration, dirt or humidity. However, the captured image is usually a high resolution one (about 500 dpi), as depicted in Figure 7.

Once the image has been captured a complex computational procedure (fingerprint image processing) must be carried out:

1. Recognition of aspects: The fingerprint is represented as a series of ‘ridges’ and ‘valleys’ with local discontinuities in the ridge flow pattern called minutiae. Galton identified four types of minutiae which were subsequently perfected and implemented.

2. Classification of fingerprints: There are four different approaches for classifying fingerprints, i.e.: • syntactic approach; • structural approach; • neural network approach; • statistical approach.

3. Matching fingerprints: The matching is the process whereby two fingerprint images are compared and the resemblance between the two geometries is measured.

### History of Biometrics

For thousands of years people have instinctively used certain physical characteristics (such as the face, voice, carriage etc) for recognizing one another. Around the mid 19th century A. Bertillon, head of the criminal identification division of the Paris Police, introduced the idea of using certain body measurements (height, length of arms, feet, fingers, etc) to identify criminals. Towards the end of the 19th century this idea was further developed thanks to the discovery (F. Galton and E. Henry’s studies) of the distinctive character of fingerprints, i.e. it was found that fingerprints are unique and therefore they bi-univocally identify a person. Following this breakthrough, police departments all over the world started to collect and store in special archives the prints of criminals, convicts and suspects. At first, these prints were “recorded” on paper by coating the subject’s fingertips with ink and creating the “stamp of the print”. Immediately after this phase, intelligence agencies and law enforcement bodies perfected techniques for collecting prints on crime scenes. Law enforcement bodies started to rely more and more on scientific investigation techniques which integrated traditional ones (deductive logic). Signs of this new “scientific approach” to investigations can also be found in literature, for example, in certain famous detective story characters (Sherlock Holmes). So, biometric science started to be used for law enforcement and anti-crime activities and also for security applications involving an ever increasing number of people. Today, in the digital era, biometric recognition techniques are very widely used not only for criminal justice purposes but also for other civilian and military applications. Some market analysts predict that by 2010 most of the earth’s inhabitants will be exposed, sporadically or regularly, to biometric recognition techniques.
The main approaches are: point by point matching and structural matching.

2.1.2 Face Recognition

Face recognition is an innate method used by humans to recognize one another. Face recognition techniques have an advantage over the other biometric techniques in that they are non invasive and require little or no cooperation from the (passive) individual subjected to recognition as they are not susceptible to behavioural modifications (voluntary or involuntary.)

Thanks to the above mentioned qualities, facial recognition technology has become quite popular in the US since the mid 1990s. From a technological point of view, besides the recent successes in the development of hardware components for image capturing (high resolution digital micro cameras), significant progress has been made in the development of recognition software.

The main technologies used for facial recognition are:
- Principal Component Analysis (PCA);
- Local Feature Analysis (LFA);
- Neural Networks.

Recognition systems should be designed according to the type of application and to the attitude of the individual. The latter may be of three types:

1. Cooperative: the subject is motivated to use the system in order to be recognised so that s/he can access portals and gates to certain areas;
2. Uncooperative: the subject does not help or hinder the recognition process;
3. Hostile or reticent: the subject tries to avoid recognition and shows evasive behaviour.

The human face is made up of a “multidimensional set of images”. From a biometric point of view, face recognition is not characterised by high permanence: the numerous facial expressions, age, the radical changes which certain features (hair, beard, moustache; etc) can be subjected to and the presence of eye glasses are examples of exterior features that can change in time and make facial recognition difficult. The ‘impermanent’ features of the face add to the complexity of the technical problems to solve. Nevertheless, successful techniques for personal identification have been developed at reasonable prices.

Facial recognition techniques are currently used mainly in verification mode comparing the facial image (captured in real time) with the (pre-recorded) image stored in the system. In identification mode the use is limited to small databases.

<table>
<thead>
<tr>
<th>Biometric Aspect</th>
<th>Fingerprint</th>
<th>Iris</th>
<th>Voice</th>
<th>Facial Geometry</th>
<th>Hand Geometry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limitations to Universality</td>
<td>Impairments or Disabilities</td>
<td>Impairments or Disabilities</td>
<td>Impairments or Disabilities</td>
<td>None</td>
<td>Impairments or Disabilities</td>
</tr>
<tr>
<td>Uniqueness</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Permanence</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Collectability</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>

Figure 3: Comparison of the Essential Requirements of Some Biometric Technologies.

Figure 4: Analysis of a Fingerprint: ‘Core’ Points and ‘delta’ Points.
2.1.3 Iris and Retina Recognition

Another Personal Identification (PI) technique uses the visible feature of the human iris. The iris is the coloured ring in the eye which surrounds the dark (black) pupil and is enclosed in the white tissue (sclera) of the eyeball (Figure 8). An iris recognition system requires a device capable of capturing the eye image (even a traditional Charge Coupled device – CCD – and the use of appropriate software which through algorithms isolates and transforms the iris into characteristic identity elements (also called templates.)

The human iris is made of elastic connective tissue which develops completely during the eighth month of gestation. The colour of the iris often changes during the newborn’s first year even though clinical studies have demonstrated that, once stabilised, the colour of the tissue remains unchanged. The iris is relatively immune to environmental disturbances except for the instinctive response of the pupil to light. A very important aspect which makes the iris particularly suitable for biometric identification is that each individual’s iris is endowed with a series of highly unique details.

Iris recognition is one of the few technologies which can be used in “identification mode”. It is quite accurate and is mainly used in security applications. It requires a certain collaboration on the individual’s part for the capture of an adequate image but, as it does not entail any physical contact, it is not an invasive procedure.

The biometric recognition of the retina is based on the uniqueness of its vascular configuration. In 1930 two ophthalmologists discovered that each human eye has a unique and stable (it does not change during the life of an individual) vascular configuration.

This system is still not widely used: to date there is only one producer of iris scanning systems. The retina is positioned inside the eye in its posterior portion. A special scanner illuminates the retina through the pupil with an infrared (IR) light and memorises the information from the reflection of vascular contrast.

Retinal scanning is considered an accurate and therefore excellent personal identification technique. Thanks to its ‘invulnerability’ it is a very effective system when absolute security is needed in access control. This technology is not easy to be applied, it requires expert operators and collaboration on the individual’s part. It is considered invasive because people usually prefer to avoid being exposed to a device that interacts with their eyes as they perceive it as potentially dangerous. This will curtail its use until a less invasive way of administering it is found. Biometric retina recognition achieves satisfactory results both in verification mode (authentication) and in identification mode. However, it is more expensive than the other methods previously mentioned. It is used and tolerated when security is a high priority but it is not suitable for large scale applications that involve a great number of people.

2.1.4 Hand Recognition

Hand geometry recognition systems measure the physical characteristics (geometry) of an individual’s hand (palm and fingers). The main technology uses a digital video camera which captures the image of the shape of both sides of the hand (palm and back). Certain geometric measurements (dimensions, length, distances, angles, etc) of an individual’s hand are calculated by the system from the ac-
Accordingly when applied to automatic processes it is usually accepted by the users more willingly than facial geometry capture and other more invasive biometric technologies.

However, the very same nature of this recognition method is also the cause that its level of accuracy is only average. In fact, the human voice has a typically physiological connotation but it is the only biometric characteristic that is also susceptible to a strong behavioural influence connected to the emotional state of the individual, which might compromise to a certain extent the uniqueness of the vocal print. Other typical behavioural features of the voice (such as speed and inflection) may contribute to a process of voice recognition.

The most widely used method for the identification of a person’s vocal print consists in analysing the frequency of sound waves resulting from the air flux generated in the lungs, spread through the tracheal duct, and brought to resonance in the larynx. If, on one hand, environmental noise and extremely different micro-phonic sensors may drastically influence the efficiency of the recording system and the verification of the vocal print, on the other hand, it is worth noting that voice recognition techniques can be easily implemented and managed using the technological resources which are normally found in most computerised structures. There is another limit of voice recognition, which makes this biometric technique better suited to personal verification and authentication in environments with a limited number of “registered users” in the database: the permanence of vocal timbre which may change in the long term due to age or physiological deterioration and in the short term due to stress, influenza and allergies.

And finally, it is worth mentioning signature recognition, that shares with voice recognition the dynamic connotation and the influence of the individual’s emotional state on performance. From the original approach which entails the assessment of the geometric differences between the signature and the registered model there has been a shift toward more advanced and dynamic techniques which take into consideration other factors such as speed, trajectory and pressure modulation during the writing process.

2.2 Personal Identification Based on Biometric Recognition of “Dynamic Aspects”

The category of the dynamic aspects of biometric recognition includes a feature which is acknowledged as one of the distinctive characters of a person: his/her voice.

Voice recognition has always been one of the most important and most natural identification methods for an interlocutor (for example, as in the case of long distance communication based mostly on voice transmission).

3. Examples of Biometric Recognition Applications

As mentioned earlier, biometric recognition technologies may be approached in two different modes: verification/authentication and identification.

In the verification/authentication mode the automatic system validates the identity declared by the subject by comparing the biometric features captured (feature extraction) with the biometric data and information prerecorded in the system’s database (template). This is called positive recognition.

In a traditional automatic system for personal identification the subject declares his/her identity through a personal identification code which can be numeric or alphanumeric (PIN – Personal Identification Number –, login or user ID). Typically, this code is manually entered to the system; it can be typed in a keyboard or read by a magnetic device or smart card owned by the subject. Authentication occurs when the correspondence between the declared identity and the password or other access code subsequently entered to the system and compatible with the access level requested by the user has been verified.

Smart cards, credit cards, and GSM (Global System for Mobile Communications) phones with access codes are all of them systems of personal accreditation. In all of these examples the identity that has been declared is verified through a comparison with the data entered to the palm device or cellular phone and the corresponding data memorised in the archive. The data transmission between the
remote terminal and the central database is carried out through a telephone line connection.

The drawback of these personal verification/authentication systems is that they are a natural target for fraud as the access code or password may be stolen or deduced and therefore used maliciously and fraudulently by an unauthorised party. In order to curtail this phenomenon and enhance the security of identity verification systems, traditional technologies may be combined with biometric recognition. In fact, the criterion underlying the security enhancement of physical access (of people) or remote systems (Internet, intranet, and business networks) is that of substituting the alphanumeric codes with the biometric features of the individual. For example, physical characteristics like fingerprints or the shape of the iris identify a person unequivocally and are difficult to forge or counterfeit.

In the following paragraphs the main applications of biometric identification technologies will be presented.

Security in computerised and physical access control: in computerized and physical access control (banks, courts, tribunals, police stations, military compounds, strategic business sectors, patent offices and Research and Development departments) security can be implemented by installing entrances with access gates (automatic sliding doors), as shown in Figure 9, and identification may be carried out by inserting a magnetic badge in specially built readers while the individual’s identity may be validated by extracting a biometric feature (fingerprint, iris, hand geometry), as shown in Figure 10). Besides physical access, biometric identification may be used to recognize the personnel who use protected computerised systems: in this case the remote terminal will be equipped for smart card insertion and extraction and processing of biometric features.

Service accreditation or accreditation with institutions: as far as service accreditation or accreditation with institutions (digital signature and biometric signature) is concerned there are legal regulations to be taken into account. For instance, according to Italian law (D. P. R. no. 513 of 1997 and corresponding bylaws) a digital signature is a system that attests to the authenticity of an electronic document (sent via Internet, e-mail, local area networks, portable memories, etc). The digital signature is gaining a foothold in document exchanges between the private citizen and the Public Administration (for example, Italian Law 340/2000 art. 31 states that all documents that firms are required to send to the Chamber of Commerce must be sent electronically and must include a digital signature) and it is expected that in the near future it will be possible to extend its use to private transactions. The digital signature, which is essentially an encryption software, is created by certain companies called certifying companies which are authorised by the Informatics Authority of the Public Administration. The certifying companies ascertain the identity of the user and provide an identity certificate and two personal keys (a public one and a private one) which are inserted in a smart card which contains in its memory all the data necessary for the identification. In order to activate the smart card the user has to enter a secret code. The certifying companies also provide a smart card reader which needs to be connected to a PC and the relevant signature software. The program derives from the text a series of characters (print) following a procedure called Hash function and using the private key it executes the ciphering of the print. The receiver who shares the same software, gets the ciphered print, the public key (that can only decode and not encrypt) and the document. S/he will apply the Hash function to the document and then compare the result with the with the received print (decoded using the public key) if the two correspond the paternity and integrity of the document are...
The introduction of certain biometric characteristics of the user (signature to the document) to be registered on the smart card so as to confirm the authenticity of electronic documents and of commercial transactions carried out via the net is currently being considered in order to enhance the security of electronic accreditation. In this context, many applications may be taken into consideration from the transmission via Internet of legal documents that guarantee the identity of the judge to the various forms of banking and e-commerce.

Anti-forgery of identity documents: the increasing need for security has prompted many countries, among which Italy, to issue electronic identification documents. Several projects are being carried out both for ID cards and passports. Smart cards can store much more than just the traditional personal information in the appropriate chip. So the data carrier technologies would make it possible to insert fingerprints or iris/retina images thus making the recognition of the user, which is traditionally based on a photograph of the subject attached to the document, much more efficient and accurate. Apart from these technical aspects, it is necessary to address another more delicate and controversial issue connected to these recognition techniques. On one hand they are extremely reliable and efficient but on the other they pose ethical problems connected to civil liberties and privacy. In December 2003 the new prototype of electronic passport was presented at Fiumicino (Rome) airport. It resembles a normal passport but a chip containing personal information, fingerprints and a photograph of the user was inserted in its cover (not visible from the outside). The main objective of an electronic passport is to avoid document forgery which is a potential threat to national security: a paper document is much easier to forge than a chip with micro processor. When the passenger arrives at the border s/he will have to place his/her electronic passport on a reading device which will verify that the data and the photograph on the document correspond to those stored on the chip. Then the subject will have to place his/her right index finger on another reader so that the fingerprints captured on site can be checked against those registered on the chip. The introduction of the electronic passport will obviously take time and require resources because it will involve all the Prefectures which will have to be equipped with the devices necessary for recording the data on the chip inserted into the passport. All international airports will need to be provided with appropriate reading devices. According to the Italian Ministry of Foreign Affairs the first new generation documents will be distributed by the end of 2004. As to the privacy and civil liberty issue, it is worth pointing out that the above mentioned system with direct on site verification (with no link to a central repository of data or central database) between the data stored on the chip and the data captured on site poses fewer ethical problems and is more acceptable in that the passport user has exclusive possession of his/her biometric data. In all the above mentioned applications authentication occurs through the on site capture of a biometric feature (fingerprints iris, etc.) and its verification either on site (storage on smart card) or through the access to a central database. Besides the verification/authentication proce-
In terms of flexibility and application reliability which might be the sign of a tendency of the current “digital reality” towards the gradual extension of such systems to increasingly numerous fields which traditionally relied on the discretion of the human operator. So, technology may lead to enhanced security and process simplification in several applications. However, even if security reasons might be a point in favour of the adoption of these systems what might curtail the implementation of such personal identification methods is the threat to privacy and civil liberties. The recent hostile reactions of American consumers to the developers of technologies capable of tracing an individual’s favourite products (through the use of radiofrequency transponders now called spy chips) are an indication that personal identity management and automatic accreditation may be perceived as an impairment on privacy when not strictly connected to security. Therefore, the way the systems are implemented and how invasive they are perceived to be, not only from a physical point of view but also in terms of the management of the collected data, become determining factors for the implementation of the available automatic ID technologies perhaps even more than their reliability.

Figure 11: Schematic Representation of the Implementation of Digital Signatures.

Translation by Giuseppina Nuzzo, Faculty of Engineering of Seconda Università degli Studi di Napoli, Italy.

Bibliography


