*e*Government and Identity Management: a Signature Coding Method for PIN generation

C. Urdiales[1], C. de Trazegnies[1], J. Vázquez-Salceda[2] and F. Sandoval[1]

[1] Dpto Tecnologia Electronica, ETSI Telecomunicacion, Campus de Teatinos s/n, University of Malaga, 29071 Malaga, Spain
cristina@dte.uma.es

[2] Institute of Information and Computing Sciences, Utrecht University, Utrecht, the Netherlands
javier@cs.uu.nl

Abstract. This paper evaluates some of the technological factors that could help to reduce the impact of *e*Government in current society. Then, ergonomics are used to provide some guidelines to design systems that could be easily accepted by users. We focus on security, which is one of the main concerns of Information Society Technologies (IST) users. Regarding ergonomics, we discuss different security options and propose a design based on biometrics, specifically on signature verification. Some preliminary tests to support the proposed design have been succesfully conducted and are also presented in the paper.

1 *e*Government and Identity Management

In recent years, the impact of technology in society is increasing. Particularly, Internet has become one of the most important links between people and technology in the last decade. *Nielsen* reports in 2002 state that a 40 % in average of people in developed countries is connected to the web. It might be of interest to note that on top of the statistics are some European contries, like Sweden (67,86 %) or Denmark (62,99 %), over countries like US (59.85 %) or China (59,55 %). It is also estimated that the percentage of connected people in countries below a 40 % will increase exponentially in the following few years.

Because of the influence of Internet, one of the best examples of the Information Society Technologies (IST), people have quickly adopted new ways of communicating both in business and in personal life. However, it has been extracted from search patterns and browsing statistics that Internet users are becoming less and less patient [12]. Nowadays, society expects information and services to be online and available around the clock in our homes, schools, libraries and work places. Government is responding to these new demands.

*e*Government is the use of IST in public administrations to improve public services and democratic processes and to support public policies. Government agencies are meant to work together to use technology so that they can better provide individuals and businesses with government services and information. Most efforts on the subject have been focused on establishing common standards

J. Padget, R. Neira, J. Díaz de León (Eds.). e-Government and e-Democracy: Progress and Challenges

across government, delivering services more effectively and providing ways for agencies to work together using technology. Basically, *e*Government is expected to deliver enhanced services to individuals in terms of efficiency, time and cost and to provide a better environment to build a knowledge-based economy and sustained prosperity. [3]

An increasing effort is currently being dedicated to *e*Government. Thus far, pilot experiences [3] have shown promising results, as residents are increasingly participating in online discussions and opinion polls about key local issues. Pilot experiences in e-voting [1] have also pointed out that IST may increase participation, particularly among young people who, traditionally, abstain from vote more that their elders. At this point, it has become clear that *e*Government is not a fashion item, but a major step forward in communications that has been accepted internationally. Hence, it is important that the government helps minimise the gap between people and IST.

*e*Government is particularly expected to be of key importance for mobility. EU-citizens are expected to travel from one Member State to another, and they will want to access and interact with public services that they are entitled to without complexities, delays and bureaucracies. Examples include access to medical services, tax submissions and rebate, access to social security services, electronic voting, pensions, identitification with authorities, etc. The government must consequently provide easy access to their rights anytime, anywhere. The mechanism for accessing those rights and meeting the obligations should be simple, straightforward, easily understandable and accessible anywhere anytime within the Member States. Citizens should also be ensured that their privacy and personal data are secure and protected, and will not be divulged into or passed on to anybody else without their authorisation.

One of the main issues to be solved in *e*Govenrment is Identity Management. Identity Management [4] is an identification mechanism to grant privacy and security to users [2]. Currently this is done mostly by paper. Electronic Identity will complement or perhaps even replace the paper-based identification by electronic means, which brings in huge advantages of availability of the information anytime anywhere. However, implementation of this raises a number of technological and organisational issues, such as security, privacy and data protection, interoperability, forms of identity management, authentication by the citizens, access of services, etc. The European Commission has been requested to propose a coherent approach to advance identity management for *e*Government.

This paper focuses on Identity Management for *e*Government applications. Authentication is not a new problem. However, if it is related to *e*Government, there are several considerations that might constraint the design of these sys-

[3] The indicative budget allocated to the Thematic Priority "Citizens and governance in a knowledge-based society" for the duration of FP6 is EUR 225 million.

[4] Identity Management is, in fact, one of the research areas proposed in FP6 for research in eGovernment. See
http //europa.eu.int/information_society/programmes/egov_rd/focus/

tems. Thus, we first analyse the factors that could have a negative impact on spreading eGovernment, specifically in the European Union (EU), from a technological point of view. Regarding these factors, several considerations related to technological design are presented in section 2. Section 3 discusses on different security options. According to the criteria presented in section 2, we focus on biometrics and, more specifically, on signature analysis. We explore current trends and describe their pros and cons. Section 4 presents a proposal to use signature for verification and automatic generation of digital PINs. In order to prove the feasibility of our proposal, a basic system is briefly outlined and tested in the same section. Finally, conclusions and future work are presented in section 5.

2 The Digital Divide, Ergonomics and Cognitive Engineering

eGovernment may be preferred by people to access government services and information for a variety of reasons: i) it may be difficult or expensive to visit a government office; ii) printed material may not be easy to obtain and keep updated; iii) traditional information might not be easy to share; and iv) queues may be avoided and time may be saved. Even though this is obviously an advantage for people living in remote areas and busy people as well, there are still some sectors of society who might be reluctant to use eGovernment. Polls (e.g., [8]) seem to point out that the most relevant factors, from the user's point of view, to adopt or not IST are cost (20 %), privacy (19 %), security (13 %) and content reliability (9 %). These polls obviously show a general concern about authentication. However, these polls usually focus on Internet users rather than on general society. From this point of view, it is also very important to take into account that some groups may be disadvantaged to benefit from IST. One risk usually associated to IST is that it may accentuate existing social divisions, a fact known as the Digital Divide (DD) [5].

The DD has been reported to present four main dimensions: political, social, economical and geographical. Politically, governments are required to grant universal access to the Information Society to citizens. Socially, DD is a function of age, gender and occupation, where the division obeys mostly to existing IST skills in population groups. Economically, it is obvious that underdeveloped countries can not deal with IST as well as rich countries. Finally, the lack of infrastructure in some areas may be a strong disadvantage to use IST. However, the greatest divide has been reported to come from education [5]: people less educated have fewer chances to use IST. Bridging the DD in well developed countries has been a challenge, but it is far more difficult in the rest of the world. Less developed countries, especially those in the south, are often plagued by limited infrastructure, low income and literacy levels, and restrictions on free expression and democratic participation. [5] Hence, strong policies are going to be

[5] See *http : //www.digitaldividenetwork.org/*

required to reduce the DD in terms of availability and affordability. Availability can be understand in terms of infrastructure, but also in terms of response to the user needs. Affordability covers not only costs but also the skills needed to access the technology.

It is a proven fact that people are adaptable. They can tolerate mild deviations from optimal designs of the equipment they use and the environments in which they work. However, there is a limit to this adaptation. Beyond such a limit, there is a cost, which can be estimated in terms of efficiency, discomfort, frustration and dissatisfaction. These problems can be avoided if an ergonomics approach is used. The word ergonomics derives from the Greek words 'ergon' (work) and 'nomos' (laws). It is an area of science concerned with the fundamental understanding of interactions among humans and other elements of a system, and the application of appropriate methods, theory and data to improve human well-being and overall system performance. Ergonomics is also referred to as human factors or human factors engineering. Given the importance of ergonomics in current technology designs, it is only natural that ergonomic factors are also used to reduce the Digital Divide. The key to ergonomics is to keep a user-centred framework [11]: it is necessary to consider persons at the centre of interest and analyze their surroundings in terms of the equipment being used, the features of the physical environment, and the social context. A user-centred approach to design and evaluation has many advantages, including: i) improved reliability ; ii) products that are easier to use; iii) better efficiency; iv) greater user comfort; v) faster learning times; vi) fewer errors; and vii) easier maintenance.

Experience with new technology has shown that increased computerization does not grant improved human-machine system performance. Poor use of technology can result in systems that are difficult to learn or use and even may lead to catastrophic errors [7]. This may occur because, while there are typically reductions in physical workload, mental workload has increased [14]: in many environments computerization has shifted the users's role from manual control of simple systems to supervisory control of highly complex, automated systems. This strong reliance on the user skills is a typical failure of design. The user's limited attention resources are shifted to the interface in order to identify desired data, configure working parameters and provide a proper feedback. Cognitive research provides insight and guidance in areas such as the effects of practice on performance, rational decision-making, and expert problem-solving in the user interface. Specifically, cognitive engineering is an interdisciplinary approach to the development of principles, methods, tools, and techniques to guide the design of computerized systems intended to support human performance [15]. A fundamental goal of cognitive engineering is to translate knowledge of human information-processing characteristics into principles and techniques for human-computer interface design [10], so that systems that are easy to learn, easy to use, and result in improved human-computer system performance. In terms of security, cognitive engineering aims at identifying unique features in the user

that he/she can provide in a simple, straight way. Thus far, most efforts have been centred either on PINs, smart cards or biometrics.

3 Biometrics for Identity Management: Dynamic Signature Verification

As discussed in the previous section, the simplest way of bringing people close to IST regarding ergonomics is to bring interfaces as close as possible to already widely accepted systems. Nowadays, the most commonly accepted identification systems to grant access to the right information or service are PINs, passwords and signatures. Smart cards are also under study. However, various competing and proprietary technologies in smart card markets pose problems for institutions interested in large-scale deployment, as there is risk of technology obsolescence or over-reliance on a single vendor. Besides, tokens, such as smart cards, magnetic stripe cards, and physical keys need to be carried and can be lost, stolen, or duplicated. On the other hand, human memory is not completely reliable: PINS and passwords consist of long strings of letters and numbers that need to be memorized and can be used by anyone. It has been recently estimated that at least 40 % of all help desk calls are password or PIN-related. Losses attributed to fraud, identity theft, and cyber vandalism due to password reliance run into the billions.

Biometric methods of identification are currently being used to replace the less secure ID/Password method of user authentication. Biometrics focus on the physical uniqueness of individuals. Once identified, significant physical features can be exactly measured, numbered, and counted. The statistical use of variations in these elements of living organisms is known as biometrics. Biometrics are particularly useful for Identity Management, in which people are recognized by biometric-based security systems according to their own unique corporal or behavioral characteristics include fingerprints, voice, face, retina, iris, handwriting, and hand geometry. Using biometric identifiers for Identity Management reduces or removes reliance on tokens. While passwords have in fact nothing to do with a person's identity and have proven to be mildly easy to decode, with biometric security the access-enabler is the person, not something he/she knows or possess. After years of research and development, biometric security systems are now in the forefront of modern security. Although public acceptance has lagged behind expectations for certain biometric applications, many concerns have been dispelled through persistent engagement and education.

Most biometric systems can be fine-tuned to work in high security or low security environments. Increasing security sometimes makes systems reject registered users, resulting in an increased False Rejection Rate (FRR). In these cases, user training may be needed. If security is set too low, though, the False Acceptance Rate (FAR) may increase. Popular biometric systems in use include iris recognition, voice recognition, and fingerprint recognition systems. Iris recognition is extremely accurate but expensive to implement and scanning the human eye is sensitive that find A typical sys-

tem is much less expensive but often exhibits unacceptably high FRR stemming from illness, hoarseness, or other throat problems. Fingerprint recognition is generally considered the most practical choice for its reliability, non-intrusive interfaces, and cost-effectiveness. However, regarding ergonomic factors, signature recognition, also known as Dynamic Signature Verification (DSV), is the least controversial of all the biometric technologies because of its natural occurrence in everyday transactions. Individuals are less likely to object to their signature being confirmed as compared to other possible biometric technologies. Besides, DSV is by far the least expensive of current biometrics on the market today. Currently, over 100 patents have been issued regarding signature verification. DSV systems are already in use in places like Chase Manhattan Bank, Internal Revenue Service (IRS), Employment Services in England, some pharmaceutical companies and visitors to Pentonville Prison in England. It is expected that DSV will become more of an everyday occurrence in society because of high public acceptance and its efficiency. DSV also presents a major advantage: even people not familiar with technologies is used to signatures for authentication and validation.

The main drawback of biometrics is that, in order to minimize the risk of loss, raw biometric data for authentication should neither be stored nor shared. Once biometric data is compiled into a database or accessible over a network, biometric information is simply data and it can be stolen. Any design based on biometrics must include the possibility that there is a loss of control over the authenticating data. Biometric systems require measures of loss recovery. The authenticating entity can control the template, and the encryption method of the biometric but never the raw authenticating data. This problem could be partially solved by separating the authentication technology from verification processes. Basically, when the user's signature is available, all parameters required for authentication are checked. Then, once his/her identity is confirmed, a feature extraction method is used to extract from the signature a stable set of characteristics that can be used as a digital PIN. This PIN does not need to be transmitted: it can be extracted by any government entity having acess to the signature and the adequate technology. It is important to note that, in this case, the PIN does not need to be memorized, is not chosen by the user and can not be forgotten because it is extracted from the signature in a straight way. Besides, since identity is already verified when the PIN is produced, forgery is not obvious. Finally, no raw biometric data is exchanged. Next section presents a rough algorithm to extract a PIN from a signature to support this proposal. It is important to keep in mind that it is not a final design but simply meant to prove the feasibility of using signatures in authentication for *e*Government applications. In order to grant the uniqueness of a given feature vector, not only global shape should be taken into account but also temporal features. Nevertheless, the proposed design would be enough for authentication in a non-global, bounded environment.

4 Verification and Digital Identity: a Signature Coding Method

DSV systems analyze two different areas of signatures: signature specific features (static) and signing specific features (dynamic) like speed, pen pressure, directions or stroke length. Some systems like UNIPEN [4] rely mostly on pen-tip velocity, but such systems are not suited for children or handwriting with tremor because they are sensitive to speed and regularity. Consequently, most systems (e.g., [9] [16]) combine both static and dynamic systems. The main drawback of static features is that the number of features to analyse is usually very large, ranging from a few dozens to hundreds. There are techniques to determine which of the features available carry more information [6]. However, even after chosing the most suitable features, it is not obvious to differentiate between the consistent parts and the behavioral parts of the signature that may change with each signing. Verification typically relies on statistically gathering enough information to grant that identification is correct despite existing feature differences. However, in order to also extract a digital ID from a signature, it is necessary to select a set of features which remain constant despite signature changes. It can be observed that strokes, angles and symmetries may change mildly from one signature to another even when they are taken from a person at consecutive time instants (Fig. 1). However, a human can easily recognize signatures belonging to the same person because they globally present the same shape. Shape has been reported to be of key importance in planar object recognition applications [13], which are typically resistant to mild local shape variations and capture condition changes. Hence, if global shape could be represented by a feature, it could be a consistent part of the signature. It is important to note that authentication must not rely uniquely on shape because, in absence of dynamic features, forgery could be easy. We propose to use both static and dynamic features in signature for authentication, like in [9] or [16], and, once the person is identified, a feature representing the global shape of the signature as a digital ID. Next subsections present a methodology to extract such a feature which has already been succesfully applied to planar object recognition [13].

4.1 Preprocessing

In order to process the shape of a signature, some preprocessing is required. First, a dilation stage is used (Fig. 2.b) to remove small discontinuities and partially soften noise. The goal of this process is to obtain a single closed shape. Then, a region growing process is performed. The seed is set at the boundaries of the image to grant that the region that grows is the background. After the background is removed, whatever remains is the global shape of the signature (Fig. 2.c).

4.2 Shape Representation

Curvature is a measure of how much the contour of a shape bends at each point. Many techniques rely on curvature to represent 2D shapes because curvature is

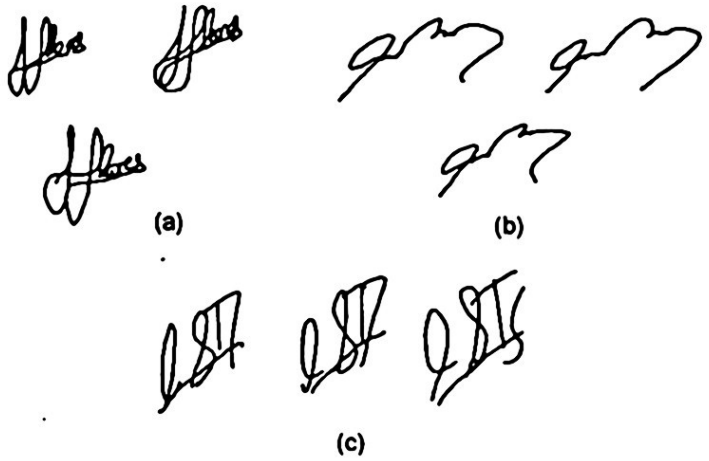

Fig. 1. Different signatures from: a) person 1; b) person 2; c) person 3.

Fig. 2. Preprocessing: a) original signature; b) dilated signature; c) region growing

usually: i) meaningful; ii) resistant to geometric transformations; iii) robust to occlusions; and iv) computationally feasible to calculate. The authors proposed a method to calculate curvature in [13] that is also very resistant against noise and adapted to the natural scale of the curve. The proposed method consists of the following steps:

- Contour encoding by means of an incremental chain code. The incremental chain code associated to a given pixel n is a vector $(\Delta x(n), \Delta y(n))$ which presents the difference in x and y between points n and $n+1$ of the contour. Further steps will represent the function by means of a code adapted to the natural scale of the curve
- For every point n, calculation of the maximum contour length $k(n)$ free of discontinuities around n. The value of k for a given pixel n $(k(n))$ is calculated by comparing the Euclidean distance from pixel $n - k(n)$ to pixel $n + k(n)$ of the contour $(d(n - k(n), n + k(n)))$ to the real length of contour between both pixels $(l_{max}(k(n)))$. Both distances tend to be equal in absence of corners, even for noisy contours. Otherwise, $d(n-k(n), n+k(n))$ is significantly shorter than $l_{max}(k(n))$. Thus, $k(n)$ is the largest value that satisfies:

$$d(n - k(n), n + k(n)) \geq l_{max}(k(n)) - U_k \tag{1}$$

being U_k a constant value that depends on the noise level tolerated by the detector.

- Calculation of the incremental adaptive chain code $(\Delta x(n)_k, \Delta y(n)_k)$, associated to n. This new vector shows the variation in x and y between contour pixels $n - k(n)$ and $n + k(n)$ and it is equal to:

$$\Delta x(n)_k = \sum_{j=n-k(n)}^{n+k(n)} \Delta x(j) \qquad (2)$$

$$\Delta y(n)_k = \sum_{j=n-k(n)}^{n+k(n)} \Delta y(j)$$

- Calculation of the slope of the curve at every point n. We consider that the slope at point n can be approximated by the angle between the segment $\overline{(n - k(n), n + k(n))}$ and the vertical axis. This angle is equal to:

$$Ang(n) = \arctan\left(\frac{\Delta x(n)_k}{\Delta y(n)_k}\right) \qquad (3)$$

- Calculation of the curvature at every point n. The curvature at every point n can be defined as the slope variation respect to n, $d(Ang(n))/dn$ This value can be approximated by the incremental $\Delta(Ang(n))/\Delta n$, or locally by $Ang(n + 1) - Ang(n)$.

Fig. 3 presents a signature and its curvature function (CF). A high point in the CF means that the curve bends a lot at such a point. Hence, corners in the signature are peaks in the function, whereas flat segments correspond to lengths of constant curvature.

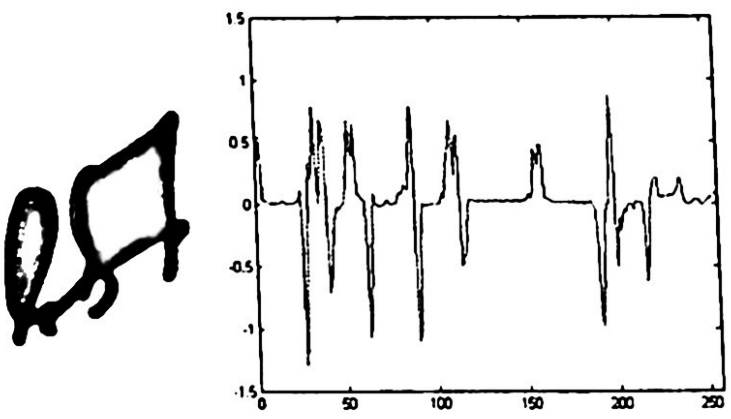

Fig. 3. A signature and its curvature function

4.3 PIN Extraction

CFs are not valid to work as PINs because: i) they may present shiftings; ii) their length depend on the signature scale; iii) they may be affected by distortions and local changes. Thus, further processing is required to achieve a stable shape feature. The authors proposed in [13] a process to reduce a curvature function to a 10 elements vector which is resistant against noise, transformations and mild distortions. First, curvatures are represented in the Fourier domain to avoid shiftings. Because of the low pass nature of the CFs, Fast Fourier Transforms of CFs (||CFFFT||s) conform a subspace of this space and its intrinsic dimension P is lower than N, being N the number of points of a ||CFFFT||. Using Principal Components Analysis (PCA), the best approximation of a ||CFFFT|| when projected onto a P-dimensional subspace is achieved by the P Principal Components associated to the P higher eigenvalues of their autocorrelation matrix. The orthogonal basis conformed by these P components, $\left\{\vec{\phi_k}\right\}_{k=1}^{P}$, is used to obtain the feature vectors for new planar shape. Given a new shape, its associated feature vector $\vec{Y}$ is obtained by projecting its ||CFFFT|| onto the proposed orthogonal basis. $\vec{Y}$ presents only P components and it is as resistant to noise and transformations as the corresponding ||CFFFT||.

$$\vec{Y} = \sum_{i=0}^{N-1} y_i \vec{\delta_i}, \tag{4}$$

In this specific case we have statistically evaluated that 10 Principal Components are enough to explain most of the variation in a signature ||CFFFT||. Fig. 4 presents different signatures from the same person and their feature vectors. It can be noted that, despite the obvious differences in strokes and proportions in the original signatures, all vectors are very similar. Thus, either any of them is used as a prototype or, after gathering some signatures, the prototype is calculated as the average of them all. This prototype becomes the digital PIN associated to the signature. Whenever a person is authenticated, both by dynamic features and vector matching, he/she receives the prototype of his/her signature as digital PIN. It can be observed that a 10 elements digital PIN is harder to hack than the usual four digit PINs currently available. It is also interesting to note that there is no need to store prototypes locally as long as a digital picture of a signature and a copy of the vector extraction algorithm is locally available. In this case, people could be authenticated by dynamic features, as proposed in [4], and vectors would be locally generated each time and matched only in reception.

4.4 Examples

In order to be useful as digital IDs, not only should vectors extracted from signatures of the same person be similar but also different from vectors of other persons. This subsection presents a simple test to show that a signature can be

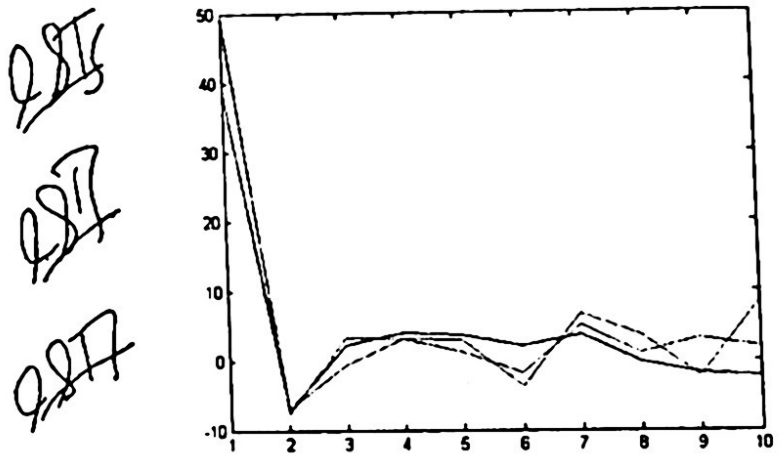

Fig. 4. Three signatures from the same person and their feature vectors.

identified using the proposed global shape feature. It is important to note that even signatures corresponding to the same person may change from time to time. Hence, the feature vectors of such signatures may also present small variations. This basically means that a signature is not recognized when a perfect match is found, but rather when the distance between the input feature vector and the signature prototype is lower than a threshold. Thus, in order to be reliable, a signature feature vector must be not only similar to its prototype but also different enough from other prototypes.

Fig. 5 presents a test with nine signatures from three different persons. Identification is correct if a signature is more similar to its prototype than to any of the other ones. It can be observed that even though signatures corresponding to the same person are globally similar, they present some differences. Fig. 5 presents the Tanimoto distances of every signature in Fig. 1 to the prototypes of the signatures of persons 1, 2 and 3 in the same figure. The dot line represents the distances to the prototype of person 1, the dash line represents the distance to the prototype of person 2 and the continuous line represents the distance to the prototype of person 3. It can be easily appreciated that all signatures from person 3 (left side of the plot) are significantly closer to prototype 3 than to the rest of the prototypes. The same occurs with signatures from persons 1 (middle of the plot) and 2 (right side of the plot). It is important to note that even though all signatures from the same person are similar, they are not equal at all: no constraints were put on persons when signatures were captured. Nevertheless, the distance between the shape vector and the prototype of each of the three persons is clearly lower when the signature is his/hers. Thus, these prototypes could be used as digital IDs as proposed.

5 Conclusions

In this paper, given the key importance of security on *e*Government, we have analysed different technological factors that might have a negative impact on the

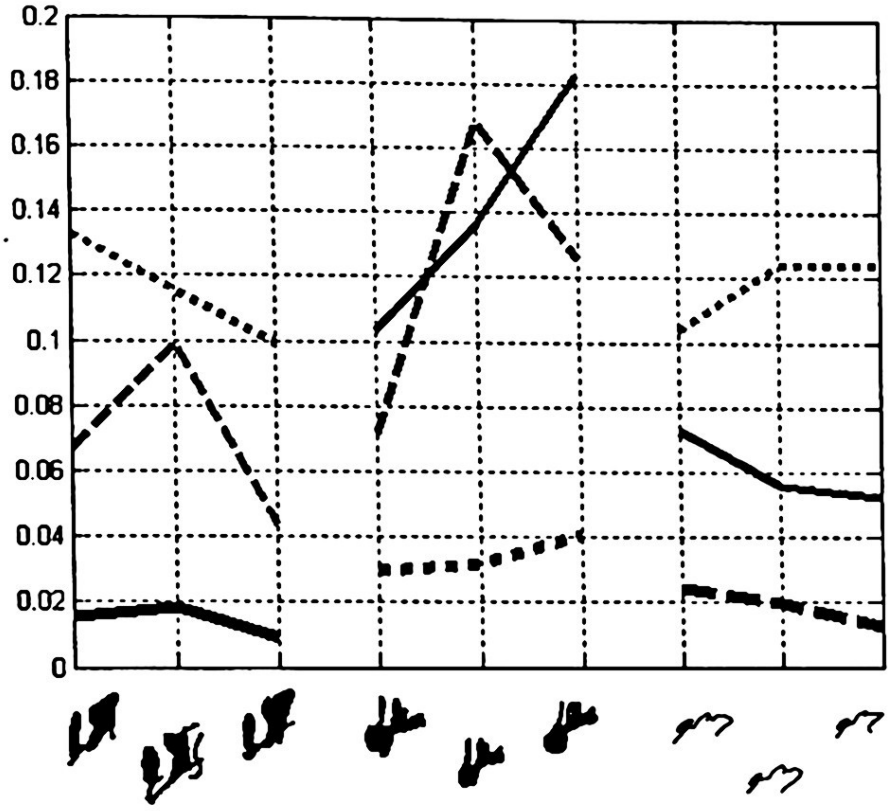

Fig. 5. Distance among each of the signatures in Fig. 1 and the prototypes per persons 1 (....), 2 (- - -) and 3 (—).

development of *e*Government initiatives. Among these factors, several studies have reported that the most important one seems to be education. Specifically, technological education seems to be required to accept IST in day to day life. Reports point out that in the EU the gap between those who may be dissadvantaged to use IST and those who are not seems to be increasing. Thus, an important effort is required to reduce that gap. Specifically, ergonomics can be applied to reduce this gap by bringing IST closer to people who may have no technological skills. Keeping all this discussion in mind, different security technologies available nowadays have been evaluated. We have focused on signature verification, which is expected to be easily accepted by users because of its natural occurrence in everyday transactions. Then, we have discussed the pros and the cons of current signature verification systems and we have proposed a technical solution to extract an stable digital ID from signatures after authentication. Finally, we have discussed the advantages of doing so. To prove the validity of the proposal, we have also outlined and tested a simple and fast algorithm to extract such an ID from the global shape of signatures. IDs in this work present 10 digits and, hence, are more difficult to hack.

Acknowledgments

This work has been partially supported by the Spanish Ministerio de Ciencia y Tecnologia (MCYT) and FEDER funds, project No. TIC2001-1758.

References

1. Barry, C., Dacey, P., Pickering, T., Byrne, D. "Electronic Voting and Electronic Counting of Votes - A Status Report", *http : //www.eca.gov.au/reports/electronic$_v$oting.pdf*, 2001
2. Camp, J.L. "The Virtual Citizen: Identity, Autonomy, and Accountability: A Civic Scenario Exploration of the Role of Identity in On-Line Governance", *Proc of the Digital Government Civic Scenario Workshop*, *http : //www.ksg.harvard.edu/digitalcenter/conference/identityReport*12_3*1.pdf*, 2003
3. Dridi, F., Pernul, G., and Sabol, T., "The Webocracy Project:Overview and Security Aspects", Schnurr, Staab, Studer, Stumme, Sure (Hrsg.), *Professionelles Wissensmanagement:Erfahrungen und Visionen*, Shaker Verlag, Aachen, pp. 401 - 408, 2001
4. Guyon, I., Schomaker, L., Plamondon, P., Libermanand, M. and Janet, S., "UNIPEN Project of On-line DataExchange and Recognizer Benchmarks", *Proc. of 12th Int. Conf. on Pattern Recognition*, pp. 29-33, 1994.
5. "The Digital Divide: a socio-economic approach", *Innovative Actions Network for the Information Society (IANIS) Newsletter*, **17**, pp.20, 2004
6. Martinez, J. and Alcantara, R. "Optimal prototype functions of features for on-line signature verification", *Proc. of the 11th Conf. of the Int. Graphonomics Society*, pp. 220-223, 2003
7. Norman,D.A., "Design Rules Based On Analyses Of Human Error" *Communications of the ACM* **26**, pp. 254-258, 1983.
8. Perez Subias, M., "Internet en España: donde estamos, hacia donde vamos", *Bit*, **130**, 2004
9. Rigoll, G. and Kosmala, A. "A systematic Comparison Between On-Line and Off-Line Methods for Signature Verification with Hidden Markov Models", *Proc. of the Int. Conf. on Pattern Recognition (ICPR'98)*", pp. 1755-1757, 1998.
10. Roth ,E.M.,Patterson, E.S. and Mumaw,R.J. *Cognitive Engineering:Issues in User-Centered System Design*, In J.J.Marciniak (Ed.), Encyclopedia of Software Engineering, 2nd Edition. New York:Wiley-Interscience,John Wiley & Sons.
11. Sanders, M.S. and McCormick, E.J., "Human factors in engineering and design", McGraw-Hill, New York, 1983.
12. Spink, A., Jansen, B.J., Wolfram, D. and Saracevic, T., "From E-Sex to E-Commerce: Web Search Changes", *IEEE Computer*, **35**(3), pp.107-109, 2002
13. Urdiales, C., Bandera, A. and Sandoval, F., "Non parametric planar shape representation based on adaptive curvature functions", *Pattern Recognition*, **35**(1), pp. 43-53, 2002.
14. Weiner, E. L., "Human Factors of Advanced Technology (Glass Cockpit) Transport Aircraft", *NASA TR 117528*, Washington, D.C., 1989.
15. Woods, D.D. and Roth, E.M., "Cognitive Engineering: Human Problem Solving with Tools," *Human Factors*, **30**, pp. 41-430, 1988.
16. Wu, Q., Lee, S., Chang, I. "On-line signature verification based on split-and-merge matching mechanism", *Pattern Recognition Letters*, **18**(7), pp. 665-673, 1997