THE "SECUREPHONE"
A Mobile Phone with Biometric Authentication and e-Signature Support for Dealing Secure Transactions on the Fly

R. Ricci
Informa s.r.l., Via dei Magazzini Generali 31, 00154, Rome, Italy

G. Chollet
GET-ENST, Dept. TSI, 46 rue Barrault, 75634 Paris cedex 13, France

M. V. Crispino
[c]Nergal s.r.l., Viale B. Bardanzellu, 8, 00155, Rome, Italy

S. Jassim
Buckingham University, Hunter Street, Buckingham, MK18 1EG, United Kingdom

J. Koreman, A. Morris
Saarland University, Postfach 15 11 50, 66041 Saarbrücken, Germany

M. Olivar-Dimas
Telefónica Móviles España S.A., Plaza de la Independencia 6, 28001, Madrid, Spain

S. García-Salicetti
GET-INT, 9 rue Charles Fourier, 91011, Évry cedex, France

P. Soria-Rodríguez
Atos Origin, c/ Albarracín, 25, 28037, Madrid, Spain

Keywords: Mobile communications, multimodal biometrics, biometric authentication, electronic signature, security, encryption, m-business.

Abstract: This article presents an overview of the SecurePhone project, with an account of the first results obtained. SecurePhone's primary aim is to realise a mobile phone prototype - the "SecurePhone" - in which biometrical authentication enables users to deal secure, dependable transactions over a mobile network. The SecurePhone is based on a commercial PDA-phone, supplemented with specific software modules and a customised SIM card. It integrates in a single environment a number of advanced features: access to cryptographic keys through strong multimodal biometric authentication; appending and verification of digital signatures; real-time exchange and interactive modification of (e-signed) documents and voice recordings. SecurePhone's "biometric recogniser" is based on original research. A fused combination of three different biometric methods - speaker, face and handwritten signature verification - is exploited, with no need for dedicated hardware components. The adoption of non-intrusive, psychologically neutral biometric techniques is expected to mitigate rejection problems that often inhibit the social use of biometrics, and speed up the spread of e-signature technology. Successful biometric authentication grants access to SecurePhone's built-in e-signature services through a user-friendly interface. Special emphasis is accorded to the definition of a trustworthy security chain model covering all aspects of system operation.

1 INTRODUCTION

Present wireless environments are not completely safe (Welch *et al*. 2003) (Torvinen, 2000). No mobile network operator can guarantee that confidential information (such as credit card numbers, personal financial data, trade secrets or business documents) can be transmitted over the air

Ricci R., Chollet G., V. Crispino M., Jassim S., Koreman J., Morris A., Olivar-Dimas M. and Soria-Rodríguez P. (2006).
THE "SECUREPHONE" - A Mobile Phone with Biometric Authentication and e-Signature Support for Dealing Secure Transactions on the Fly.
In *Proceedings of the International Conference on Security and Cryptography*, pages 9-16
DOI: 10.5220/0002103900090016

in a secure way. Likewise, it is often not possible to reliably verify a user's identity, due to the absence of trustworthy strong authentication procedures. Security and dependability are essential prerequisites for the spreading, for instance, of mobile e-business (m-business) applications, especially where legal aspects play an essential role. In synthesis mobile infrastructures should provide the following four major security services:

- Authentication (verification of the user's identity by remote).
- Confidentiality (privacy)
- Non-repudiation (signing in a verifiable way at a later stage).
- Integrity (sealing: during transmission and after a signed digital agreement).

It is expected that a combination of Public Key Infrastructure (PKI) technology and biometrics can play a key role to enhance wireless environments safety by ensuring identity and protecting information.

In this article we present an original solution, developed in the context of the SecurePhone project (an international project co-funded by the European Commission started in 2004). The SecurePhone is an innovative prototypal mobile phone platform that gives users the possibility to authenticate by means of a multimodal "biometric recogniser", exchange, modify in real time and finally e-sign and securely transmit audio and/or text files. The biometric recognition is based on three modalities: voice, face and handwritten signature recognition.

In section 2 we describe SecurePhone's main objectives and system architecture. Section 3 briefly presents the biometric recogniser and the method used for score fusion. Section 4 reports preliminary results of the project. In section 5 we present some ideas for future developments. Conclusions are given in section 6.

2 SECUREPHONE SYSTEM ARCHITECTURE

The aim of the SecurePhone project is to enable biometrically authenticated users to send/receive files via a mobile phone in an easy yet highly dependable and secure way.

The typical case of use considered in the project is that of two users (the proposer and the endorser) who directly exchange, eventually agree upon and e-sign a digital document (e-contract):

- the proposer sends to the endorser the e-contract - either a text or a digital audio file;
- the e-contract – at least in the case of a text file - is modified and transmitted back and forth between the two users as many times as needed to reach a formal agreement on its contents;
- the endorser eventually e-signs the e-contract and sends it to the proposer as an evidence of formal acceptance of the contract terms. Depending on the contract type, the proposer could also be requested to e-sign the e-contract;
- just before that the e-signature procedure is initiated, the host application running on the PDA asks the user to pass an authentication challenge, in order to "unlock" the e-signature private key located on the SIM card and get access to built-in cryptographic services.

It is assumed that the private key of the SecurePhone's owner - needed for e-signature and other cryptographic tasks - is safely placed on the SecurePhone's SIM card, which, besides supporting normal telephonic services, also provides the possibility of tamper-proof data storage.

The SecurePhone can also be adapted to be used in a User/Business model, in which a single user accesses some business service provider over a private or public network.

In the use case described above the authentication challenge, which gives access to the private key stored onto the SIM, is the crucial phase of the process. In normal practice, authentication is done by inputting a password or a PIN. This is considered a weak authentication modality, that is not particularly suited for critical applications such as e-commerce.

In order to strengthen the user authentication procedure we decided to use a multimodal biometric identity verification.

2.1 Biometric Verification Architecture

Biometrics identity verification can be implemented by adopting different architectures (Petterson *et al.* 2002), namely:

- Match-on-Card (MoC): verification is performed by an applet running on the SIM card. This scheme implies Template-on-Card (ToC), i.e. the reference biometric templates must also be stored on the SIM card.
- Match-on-Host (MoH): verification is performed by a trusted application running on the host (the PDA, in our case). ToC is also

usually implied in this scheme, for privacy reasons (Bella *et al*., 2003).

- Match-on-Server (MoS): verification is performed by an application running on an on-line Trusted Third Party (TTP) server. In this scheme, Template-on-Server (ToS) is usually implied, i.e. the reference biometric templates must also be stored on the TTP server.

MoC has been adopted as the SecurePhone's primary biometric identity verification architecture, because of the high levels of security and privacy that it permits to attain - at least on theoretical grounds. MoH was also implemented as a testbed for the assessment of MoC verification results.

The MoS model was discarded because it deviates strongly from SecurePhone original concept and because of privacy considerations, which present arguments against the use of central servers for the storage of sensitive data like biometric templates. Furthermore, MoS does not seem to ensure adequate security levels for the purposes of the SecurePhone project, if not at the cost of implementing a complex network architecture exploiting cryptographic technology for securing the communications between the various entities involved.

2.2. Hardware Requirements

In terms of hardware, the choice has been made to use a commercial "off-the-shelf" mobile phone without any particular add-ons. At the moment of selecting the most suitable platform – early 2004 – the best choice resulted in the selection of the Qtek 2020 a GSM/GPRS PDA-phone - also known as O2 Xda II, SPV M1000 - manufactured by the Taiwanese company HTC under the generic nickname of "Himalaya". Since GPRS technology does not enable the simultaneous transmission of voice and data during a single session, some limitations descended from this forced decision that had an influence on service design. Another drawback, in terms of usability and intrusiveness, is related to the fact that the Qtek 2020 built-in camera is on the rear of the device, thus making the capture of audio-video data more cumbersome. A new UMTS PDA-phone (the Qtek 9000, a.k.a HTC Universal) has recently been launched on the market that will make it possible to overcome these technical limitations.

Although the SecurePhone is in all respects a normal PDA-phone, the SIM card that it uses is special, since it must provide built-in support for symmetric and asymmetric cryptography and enough storage space for the needs of MoC biometric authentication. The SIM card selected for the project is a GSM-compatible, PKI Java card with 128 KB RAM, providing support for RSA and ECC crypto-algorithms.

2.3 System Architecture

A high-level representation of SecurePhone system architecture is given in Figure 1.

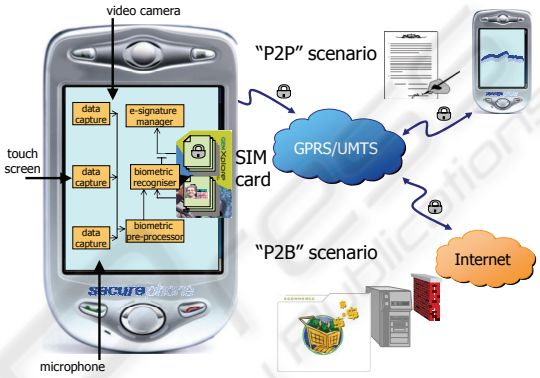

Figure 1: system architecture and service models.

All communications between host applications running on the PDA and applets on the SIM card are compliant with the Application Protocol Data Unit (APDU) protocol, defined in ISO-7816 part 4 for communications with card-based applications.

The functionalities of the specific software modules required for system operation are briefly described in the following subsections.

2.3.1 Software Modules on the PDA-phone

- Document Exchange Module
  This module is a fundamental part of the SecurePhone user interface. It enables to:
  - produce an e-contract - or import it from a list of predefined document templates;
  - transmit the e-contract to another SecurePhone device over the GPRS network and receive it back in a possibly modified form;
  - modify a received e-contract interactively in order to produce a final form the two users agree on;
  - launch the Authentication Module for biometric authentication against the device - once an agreement on the contents of the e-contract has been eventually reached - in order to verify the identity of the user who is required to e-sign;

- request the e-Signature Module to e-sign the e-contract, if the user's identity has been verified;
- request the e-Signature Interface Module to verify the e-signature on an e-contract.

- Authentication Module
  This module is responsible of:
  - acquiring a user's "live scan" biometric samples by means of the device sensors (video camera for face, microphone for voice and touch screen for handwritten signature);
  - pre-processing the acquired biometric samples in order to produce live scan biometric parameter vectors;
  - sending live scan biometric parameter vectors to the SIM card for comparison with enrolment biometric models stored therein.
- e-Signature Interface Module
  This module interfaces the SIM card for all tasks related with the creation of e-signatures, namely:
  - produce a digest of the e-contract;
  - randomly create a symmetric key and use it to encrypt the e-contract;
  - transmit the digest and the symmetric key in a single bundle to the SIM card in order to have it e-signed;
  - verify the e-signature on an e-contract and retrieve the symmetric key used to encrypt it;
  - decrypt the e-contract with the retrieved symmetric key.

2.3.2 Software Modules on the SIM Card

- Biometric Verification Applet
  This module is implemented as a Java applet and enables to:
  - compare live scan biometric parameter vectors with enrolment biometric models that are securely stored onto the SIM card itself, using a verification threshold for each individual modality;
  - apply a fusion algorithm to the verification scores obtained by each single biometric modality, in order to produce a single value to be verified against a threshold;
  - produce the pre-specified "unlocking" code that is required to enable SIM card cryptographic services in case of successful authentication.
- e-Signature Applet
  This module is implemented as a Java applet and is responsible of:
  - generating and managing cryptographic keys on the SIM card;
  - controlling the data sent and received with the e-Signature Interface Module running on the PDA during a data transfer session;
  - recombining data received during a single session;
  - performing the cryptographic operations involved in electronic signature creation.

3 THE "BIOMETRIC RECOGNISER"

SecurePhone's innovative biometric recogniser plays an important role in ensuring the overall dependability of the proposed solution.

The choice has been made from the outset to exclude biometric identification modalities that may have social connotations – e.g. fingerprint recognition. Psychological discomfort is in fact the first cause of social resistance to biometrics for identity verification applications. The SecurePhone solution exploits three biometric modalities – namely voice, face and handwritten signature recognition – chosen because of their non-intrusiveness and friendliness to users as "natural" identification means. Another important factor that influenced the choice of these biometrics is that commercially available PDA-phones are already equipped with reasonably good sensors to capture the relevant biometric data, so that no extra dedicated hardware is required.

The three modalities are fused in a single biometric recogniser, which has been specifically designed and developed as a result of extensive original research. In particular the fusion scheme has been optimised so as to enhance verification performance and provide robustness to changing environmental conditions.

As a further security measure, the biometric templates used to authenticate a device's legitimate owner are stored on the device SIM card during the enrolment phase and never leave the card during system operation. Since biometric verification is performed on card, special care was required to efficiently adapt biometric algorithms to the reduced computational and memory resources provided by currently available SIM cards.

3.1 Data Modelling

Due to their inherent variability, all three of the biometrics modalities selected require the use of statistical data models rather than simple templates.

While state of the art models differ between modalities, we have found that Gaussian mixture models (GMM) (Duda *et al*., 2001), used together with a GMM universal background model (UBM), give performance which is close to state of the art for all three modalities. While this is the model of choice for voice based authentication (Reynolds *et al*., 1995), the high performance which this model also gave for face and signature verification was unexpected. This is probably because for all three modalities the amount of enrolment data available for model training is very restricted. The GMM with MAP adaptive training (updating the Gaussian means only) from a UBM is well suited to small amounts of training data. The UBM serves two purposes. It is used to initialise the client model before adaptive training with the enrolment data, and it is also used as a universal impostor model for score normalisation (the score used is proportional to the logarithm of the ratio of the posterior client probability to the posterior impostor probability). All three modalities on the PDA use a GMM to model biometric data features. Models were trained using the Torch machine learning API (Collobert *et al*., 2002). A UBM, pre-trained on data from a number of speakers, is installed both on the PC where enrolment takes place, and on the SIM card. Enrolment then comprises 8 simulated client accesses, during which time the lighting and background noise conditions are varied to reflect the range of conditions expected during use. After biometric features have been extracted from this data, these features are used to train a GMM client model for each modality, which is then installed on the client's SIM card (Koreman *et al*., 2006).

3.2 Face Verification

There are many different face verification schemes. For efficiency required by mobile devices, wavelet-based verification schemes were selected for investigation and development. Wavelet transforms are multi-resolution image decomposition techniques that provide a variety of channels, representing the image features by different frequency subbands at different scales. Various combinations of wavelet filters, frequency subbands, and levels of decomposition were developed for implementation on the adopted PDA. Several lighting normalisation procedures were also investigated, since they can substantially improve face recognition under the variable conditions in which the SecurePhone is used. The performances of some of these schemes were extensively tested on a number of benchmark biometric databases as well as on a newly created audio-visual database (the "PDAtabase").

The PDAtabase was primarily designed to test fixed-prompt based user authentication on the QTEK 2020, using biometrics from voice, face and handwritten signature. Video data was recorded, using the PDA-phone, from sixty English speaking subjects (80% native) at 44 kHz audio and 20 frames per second video. Each subject was recoded in two well separated sessions. Each session was recorded under two different inside lighting and noise conditions and two different outside conditions. Six examples of each of three different prompt types were recorded under each condition (5 digits, 10 digits and short phrases). Signature data was recorded from sixty separate subjects. Each subject recorded twenty repetitions, and was impostorised twenty times (by one other person).

For more details on the face biometric, testing experiments and the PDAtabase we refer the reader to (Morris *et al*., 2006) (Sellahewa *et al*., 2005) (Sellahewa *et al*., 2006).

3.3 Speaker Verification

Voice features use 19 Mel-frequency cepstral coefficients (MFCC, without c0), with cepstral mean subtraction (CMS) to remove convolutive noise, and non-speech removal to reduce uninformative data. First order time difference features are then added (Reynolds *et al*., 1995). All processing is online, so that feature processing can start before the utterance has been completed. While the PDA is capable of sampling at 44 KHz, sampling was set to 22 KHz as this reduces processing time without compromising verification accuracy.

3.4 Handwritten Signature Verification

Signature data is captured from the PDA touch screen at 100 (x,y) samples per second. This sequence of 2 dimensional data is then processed to give a sequence of 19 dimensional feature vectors (Dolfing, 1998). The glass touch screen is not an ideal surface for writing on. PDAtabase tests (signatures of 64 different writers acquired by using the Qtek 2020) showed that signatures obtained in this way could give good verification accuracy, but not as good as signatures obtained from a dedicated writing tablet which also measures pen pressure and two pen angles (Garcia-Salicetti *et al*., 2003).

3.5 Fusion

Each of the three biometric modalities can be used separately to perform the identity verification, but the combination of the three systems has several advantages. Firstly, multimodality is expected to strongly enhance person authentication performance in real applications as shown in (Allano *et al*., 2006). Secondly, operational conditions generate degradations of input signals due to the variety of environments encountered (ambient noise, lighting variations, …), while the low quality of sensors further contributes to decrease system performance. By fusing three different biometric traits, the effect of signal degradation can be counteracted.

In order to combine several biometric modalities, fusion can be performed at different levels: feature level, score level or decision level. Many fusion techniques have so far been compared in the literature. In (Allano et al., 2006), two types of score fusion methods have been compared on the PDAtabase (Morris, Koreman, Sellahewa, Ehlers, Jassim, Allano, Garcia-Salicetti, 2006) (Morris, Jassim, Sellahewa, Allano, Ehlers, Wu, Koreman, Garcia-Salicetti, Ly-Van, Dorizzi, 2006). The first type is based on the Arithmetic Mean Rule after a previous normalization of each score separately. The second type is based on modelling the 3D distribution of client and impostor scores, for example using a Gaussian Mixture Models (GMM). After testing a number of different fusion methods suited to the limited computing capability of the PDA, the method selected for implementation was GMM based fusion (Allano et al., 2006) (Koreman et al., 2006). In this model, during enrolment two scores GMMs are installed in the PDA. One is trained to model the joint distribution of client scores and one the joint distribution of impostor scores. These scores GMMs were first trained on a large amount of scores data by combining data from all six of the 5-digit prompts tested, and then retrained on data from the single prompt selected for use in the working PDA, updating the Gaussian means only. During verification the client match scores from each modality are concatenated into a single vector and from this the client-scores GMM estimates a client log likelihood and the impostor-scores GMM estimates an impostor log likelihood. The difference of these log likelihoods provides a log likelihood ratio, which is the combined score against which the accept/reject decision is made using a suitably estimated threshold.

3.6 Forgery Scenarios

As with any security system, the level of security depends on the effort which an impostor is prepared to invest. In the case of the present fixed prompt system with static face recognition, if a photograph of the owner's face and signature together with a high quality recording of their reading the fixed prompt was obtained, then successful impostorisation would be possible. This imposture scenario could be avoided if it were feasible to implement the liveness test proposed in (Bredin *et al.*, 2006), in which a check is made on the degree of correlation between mouth opening and speech energy. However, the present PDA is not capable of the computation required for mouth tracking. Such issues may require the development of suitable dedicated hardware (Koreman *et al*., 2006).

Table 1: EER, FAR and FRR % scores (for 3 typical values of the false acceptance to false rejection cost ratio, R) obtained with the PDAtabase. Scores were obtained using a threshold optimised for data from one set of speakers while testing on another set. For test details, see (Morris, Koreman *et al*., 2006).

	EER	FAR			FRR		
		R=0.0	R=1.0	R=10.0	R=0.0	R=1.0	R=10.0
Voice	6.12	19.10	4.81	0.86	2.08	8.33	19.10
Face	28.57	93.77	26.44	1.18	1.16	30.44	85.53
Signat.	6.19	13.61	6.94	4.31	2.78	4.86	52.78
All 3 fused	0.85	2.15	1.90	0.39	0.81	1.16	3.94

4 RESULTS

Although the SecurePhone project has not been finished yet, a first prototype of the system has been implemented and is under evaluation at the moment of writing. The prototype includes the module for document exchange as well as a first release of the authentication module (biometric recogniser), which is presently running on host (MoH biometric verification). The MoC verification applet is in advanced development phase, while the e-signature applet has been fully implemented and is currently under test in a simulated environment, before final deployment on the SIM card.

Prior to implementation on the PDA, the performances of the biometric recogniser were thoroughly investigated on a desktop workstation in an environment that closely emulates the operational conditions expected on the mobile device. Table 1 shows test results obtained from a database which was recorded on the PDA (Morris *et al*., 2006). Results are averaged over separate tests for six different 5-digit prompts. The prompt with the best score ("28376") was used in the PDA. 10-digit prompts lower the fused average EER from 0.85% to 0.56%, but 5-digit prompts reduce preprocessing time. Further reduction in error rate could be obtained if more memory was available for biometrics model storage. Voice, signature and face models presently require 23.0, 2.9 and 11.6 Kb respectively. Tests run directly on the PDA are in progress at the moment of writing..

Figure 2: A screenshot of the SecurePhone system prototype.

Figure 3: SecurePhone system prototype.

5 FUTURE DEVELOPMENTS

The very promising results obtained so far in the SecurePhone project encourage us to investigate their possible exploitation in various directions. The primary effort will be to further improve the performances of the biometric recogniser and implement other operation modes. Present restrictions in terms of user interface and overall usability will be overcome in the immediate future by the adoption of the recent Qtek 9000, running Windows Mobile 5.0, with integrated UMTS support and a CIF camera in the front.

Another line of development that is presently under investigation is focused on exploiting the SecurePhone biometric technology to realise a "seamless recogniser". The idea is to use combined face and speaker recognition in the initial phase of a video call for the mutual identification of the two parties involved in the video call itself, who do not need to know each other personally. A success in mutual identification could seamlessly trigger the encryption of the communications between the two parties. Such a system can find countless applications in all sectors where high levels of trust and confidentiality are required – intelligence, the military, safe communication of trade secrets, etc.

A further, more visionary step in the development of SecurePhone outcomes extends the concept of biometric multimodal identification beyond the scope of mobile communications, by realising a multiplatform biometric recogniser suitable to be used in general network applications. This idea is closely related to current research on identity management for universal access, an emerging field in information and communications technology.

6 CONCLUSIONS

The vision embodied in the SecurePhone project is to reduce the psychological intimidation often felt by ordinary users towards new ICT technologies by proposing new advanced uses for a familiar and intuitive communication platform such as the mobile phone. Although supplemented with high-tech functionalities, the SecurePhone does not differ from a common PDA-phone in terms of ease of use and user-friendliness. Under its surface appearance, though, a remarkable level of innovativeness is hidden: by means of the SecurePhone users will be given the opportunity to draw legally valid e-transactions, relying on the security provided by electronic signature for a whole new set of possible social interactions and business opportunities.

This work was supported by the EC SecurePhone project IST-2002-506883

REFERENCES

Allano, L., Garcia-Salicetti, S., Ly-Van, B., Morris, A.C., Koreman, J., Sellahewa, H., Jassim, S. & Dorizzi, B., 2006, "Non intrusive multi-biometrics on a mobile device: a comparison of fusion techniques", *Proc. SPIE conference on Biometric Techniques for Human Identification III*, Orlando, 2006.

Bella G., Bistarelli S., Martinelli F., 2003, "Biometrics to Enhance Smartcard Security (Simulating MOC using TOC)", Proc. 11th International Workshop on Security Protocols Cambridge, England.

Bredin, H., Miguel, A., Witten, I.H. & Chollet, G., 2006, "Detecting replay attacks in audiovisual identity verification", *Proc. ICASSP* 2006 (in print).

Collobert, R., Bengio, S. & Mariéthoz, J., 2002, "*Torch: a modular machine learning software library",* Technical Report IDIAP-RR 02-46.

Dolfing, J.G.A., 1998, "*Handwriting recognition and verification, a Hidden Markov approach*", Ph.D. thesis, Philips Electronics N.V.

Duda, O., Hart, P.E. & Stork, D.G., 2001, *Pattern classification,* Wiley.

Garcia-Salicetti, S., Beumier, C., Chollet, G., Dorizzi, B., Leroux-Les Jardins, J., Lunter, J., Ni, Y. & Petrovska-Delacretaz, D., 2003, "BIOMET: a Multimodal Person Authentication Database Including Face, Voice, Fingerprint, Hand and Signature Modalities", *Proc. 4th Conf. on AVBPA*, pp. 845-853, Guildford, UK..

Koreman, J., Morris, A.C., Wu, D., Jassim, S., Sellahewa, H., Ehlers, J., Chollet, G., Aversano, G., Bredin, H. Garcia-Salicetti, S., Allano, L. Ly Van, B. & Dorizzi, B., 2006, " multi-modal biometric authentication on the SecurePhone PDA", *Proc. MMUA*, (in press).

Morris, A.C., Jassim, S., Sellahewa, H., Allano, L., Ehlers, J., Wu, D., Koreman, J., Garcia-Salicetti, S., Ly-Van, B., Dorizzi, B., 2006, "Multimodal person authentication on a smartphone under realistic conditions", *Proc. SPIE conference on Mobile Multimedia/Image Processing for Military and Security Applications",* Orlando, 17-21 April, 2006.

Morris, A.C., Koreman, J., Sellahewa, H., Ehlers, J, Jassim, S., Allano, L. & Garcia-Salicetti, S., 2006, "*The SecurePhone PDA database, experimental protocol and automatic test procedure for multimodal user authentication*", Tech. Report, http://www.coli.uni-saarland.de/SecurePhone/documents/PDA_database_and_test_protocol.pdf

Pettersson M., Obrink Ä, 2002, "*How secure is your biometric solution?"*, Precise Biometrics White Paper, http://www.ibia.org

Reynolds, D.A., 1995, "Speaker identification and verification using Gaussian mixture speaker models", *Speech Communication, Vol.17,* pp.91-108

Sellahewa, H. & Jassim, S.,"Wavelet-based Face Verification for constrained platforms", 2005, *Proc. SPIE on Biometric Technology for Human Identification II*, Florida, Vol. 5779, pp 173-183.

Sellahewa, H. Al-Jawad, N., Morris, A.C., Wu, D., Koreman, J. & Jassim, S., 2006, "Comparison of weighting strategies in early and late fusion approach to audio-visual person authentication", *Proc. SPIE conference on Mobile Multimedia/Image Processing for Military and Security Applications",* Orlando, 17-21 April, 2006.

Torvinen V., 2000, "Wireless PKI: fundamentals", Radicchio white paper, http://www.radicchio.org

Welch D. J., Lathrop S. D., 2003, "A Survey of 802.11a Wireless Security Threats and Security Mechanisms", Tech. Report, ITOC-TR-2003-101, http://www.itoc.usma.edu/Documents/ITOC_TR-2003-101_(G6).pdf