# MOBIO

## Mobile Biometry

http://www.mobioproject.org

Funded under the 7th FP (Seventh Framework Programme)
Theme ICT-2007.1.4
[Secure, dependable and trusted Infrastructure]

# D2.1: Report on the use cases scenarios and general functional requirements for biometry-enabled telecommunication system

| | |
|---|---|
| **Due date**: 30/04/2008 | **Submission date**: 19/12/2008 |
| **Project start date**: 01/01/2008 | **Duration**: 36 months |
| **WP Manager**: Christopher McCool | **Revision**: 12 |

**Author(s)**: Giorgio Zoia (EPM)

| | | |
|---|---|---|
| **Project funded by the European Commission<br>in the 7th Framework Programme (2008-2010)** | | |
| **Dissemination Level** | | |
| PU | Public | No |
| RE | Restricted to a group specified by the consortium (includes Commission Services) | Yes |
| CO | Confidential, only for members of the consortium (includes Commission Services) | No |

# D2.1: Report on the use cases scenarios and general functional requirements for biometry-enabled telecommunication system

**Abstract:**

This deliverable specifies a variety of use cases for biometry-enabled telecommunication systems, with an emphasis on the role of mobile devices.

The precise identification of the use cases is necessarily based on a) an analysis of current telecommunication applications, which already make use of biometric authentication technology; b) an analysis of current telecommunication systems in terms of network capabilities and available services, and finally c) a review of existing and next-generation mobile devices.

The deliverable fully specifies five major use case scenarios selected from a number of identified customer and telecommunication industry needs. They span over a wide range of real life situations, from high security bank transactions to every-day entertainment, showing the big impact that biometric-enabled telecommunication systems, and consequently MOBIO, may have on the security and comfort of people. The basic technology and functional requirements are identified by these use cases.

# Table of Contents

# 1.Introduction

These days, portable personal devices (PDAs and mobile phones) are widely used. They provide the mobile worker or the general customer with portable computing and wireless access to telecommunication networks and to the Internet. It is then possible to provide anywhere anytime a natural access to services such as phone card reloading, remote purchase, telephone banking or voice-mail. Most of these services involve micro payments that require the user to authenticate their identity.

To win wide consumer acceptance these services need friendly, personalized, interactive interfaces that are able to recognize, or authenticate, people in their immediate environment. The conventional method to authenticate a user is to have a password, secret code or personal identification number (PIN). These conventional methods of user authentication can easily be compromised, shared, observed, stolen or forgotten. By contrast biometric authentication methods, which recognize a person using their own distinguishing traits such as their face, provide a natural and unintrusive way to authenticate a person's identity. In view of this, MOBIO focuses on authenticating the identity of a person using easily obtained biometric information such as the face and the voice.

The goal of this project is to study, develop and evaluate bi-modal biometric authentication technologies in the context of portable devices and related network infrastructures. More particularly, MOBIO focuses on two natural and unintrusive biometric modalities, namely face and voice. The face is considered because it is a socially accepted biometric that is used extensively in passports and identity cards across the world, it is also biometric information that can be easily be obtained as most mobile devices now have at least one camera. The voice is considered as it is naturally and readily available from mobile devices such as mobile phones, also, voice authentication is a mature field of research.

Bi-modal biometric authentication on portable devices such as mobile phones is a challenging task. By definition a mobile system operates in an uncontrolled and unconstrained environment and thus the data captured can be very noisy (background noise in the audio signal, strong and non-uniform illumination in the video signal). This leads to the scientific and technical objectives of the project which include: robust-to-illumination face authentication, robust-to-noise speaker authentication, joint bi-modal authentication, model adaptation and scalability. In addition to these objectives there are other fundamental issues that it is hoped MOBIO will be able to address.

A fundamental concept that is being developed by an increasingly global society is that of convergence. Convergence is considered to be the transparent availability of services in different times and places accessed by different devices through various networks. It is difficult to envisage how a single conventional authentication method, such as a single PIN, will address authentication in this complex situation. However, biometric authentication could provide an elegant solution to authentication in a convergent environment. This is because biometric authentication provides a transparent means of authentication that is similar to how a human authenticates the identity of a person; by using the available biometric information. In fact, using biometric authentication means that the user can interact in the same way to any interface without having to remember the particular password or PIN. For these reasons it is foreseen that mobile-based biometric authentication can play an important role for convergence to be realized. The concept of convergence also highlights the broad range of use cases that MOBIO could address.

The use cases considered in the MOBIO project need to meet three criteria. The first criterion is that the use case must meet the needs of the consumer. The second is to meet the needs of the market and the final criterion is that the use case is possible with currently available technology. These three criteria are considered in the following sections by reviewing the current trends of both the market and the consumer and also by doing an extensive review of the currently available mobile devices.

The remainder of this deliverable is organized as follows. The current state of biometrics in telecommunication applications is reviewed. Following this the current telecommunication scenarios are described and then the state of the art in mobile devices is provided. The use cases for the MOBIO project are then described in detail and the functional requirements for the mobile device are then defined. To conclude, the fundamental aspects of this deliverable will be summarized with final remarks on the device choice.

This second review of the deliverable considers in greater detail aspects related to threat and security scenarios. In particular, each use case includes a short analysis of trust and threat models along with the security mechanisms that will be applied to them. This document also emphasizes the IP Multimedia Subsystem (IMS) architecture aspects, which implicitly addresses security and encryption issues.

# 2.State-of-the-Art Biometric Applications in Telecommunication Applications

This section provides an overview of the biometric authentication technologies which are currently available in the telecommunication domain. It also highlights the innovative contributions that MOBIO will make.

## 2.1.Technologies and Applications

MOBIO focuses on multiple aspects of biometric authentication ranging from research to development and scalability. This is all considered in the context of a mobile environment and consequently is based on natural and unintrusive modalities such as face and voice. The face and voice are considered to be natural and unintrusive modalities as mobile phones are catering specifically for these two modalities. This is shown by the increasing number of mobile devices which are equipped with a frontal camera to allow for video calls, see Figure 1. There are other biometrics that could be applied to mobile devices, however, the other biometrics are often intrusive.

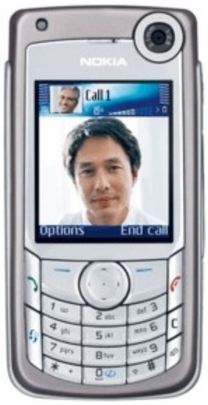


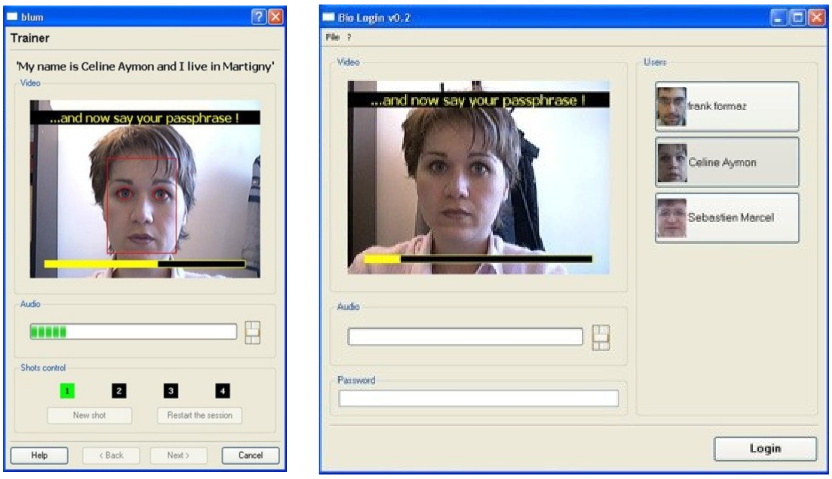
*Figure 1. An example of a mobile device equipped with a built-in frontal video camera.*

Other biometrics such as fingerprint and iris are intrusive and require active participation by the user. This is reflected by the fact that there very few devices which are equipped with a fingerprint scanner and no known mobile device with an iris scanner. However, the apparent lack of a more natural biometric has led some manufacturers to equip their mobile devices with a fingerprint scanner, some examples are: Fujitsu DoCoMo F902i, Pantech PG-6200, Radio Co. WX310J, Porsche P9521, Hitachi W51H, Willcome WX321J, LG LP3800 and HLS 9100.

There are very few companies that provide mobile biometric authentication technologies that make use of built-in sensors; for instance using audio and video. So far only Omron in Japan, Persay (for speech) in Israel, VeriVoice (only for speech) and Nevenvision in the US have claimed such capabilities. It should be noted that Nevenvision was recently acquired by Google.

The lack of bi-modal authentication systems on mobile devices is surprising given the current state of bi-modal authentication. There are several state-of-the-art bi-modal authentication systems which are currently available, these include:

- **Bi-Modal Login**: a bi-modal authentication system (running both Linux and Windows operating systems) which is freely available. For more details, the reader is referred to the demonstration web page (http://www.idiap.ch/biologin), an example of this system is provided in Figure 2.
- **Viola-Jones face detection on a mobile phone**: the face detection framework proposed by Viola and Jones has been implemented on a mobile phone, see Figure 3) Indeed, several of the MOBIO partners (IDIAP, UOULU, BUT, EPM) have experience in the development of audio and visual processing systems on mobile phones.



'My name is Celine Aymon and I live in Martigny'

...and now say your passphrase !

...and now say your passphrase !

*Figure 2. Bi-Modal Authentication system based on face, speech and fusion developed at IDIAP. The system provides a BioLogin application (left) to test a client, and a Manager application (right) to create a new account by enrollment.*

- **BioSign**: an example of a remote bi-modal biometric system. It is based on a simple client/server architecture (Figure 4), where the mobile device acts as the client. The main objective of this system is to evaluate the performance of state-of-the-art bi-modal biometric authentication algorithms in a mobile environment. The mobile device was only used for data capture and transmission to the server. The authentication, segmentation (except face localization performed on the mobile device using the previously described Viola-Jones implementation), preprocessing and feature extraction was hosted on a server.

| | **PC** | **Nokia 7650** | **Sony-Ericsson P900** |
|---|---|---|---|
| Processor | Pentium IV | Arm 9 core | Arm 9 core |
| CPU clock (MHz) | 2660 | 104 | 156 |
| Processing time (ms/frame) | 8.2 | 210 | 260 |
| Image size (width x height) | 384x288 | 192x144 | 192x144 |

*Figure 3. Viola-Jones face detection running on a Mobile Phone. The table on the right shows the processing time (including capture, face finding and display) on several architectures.*

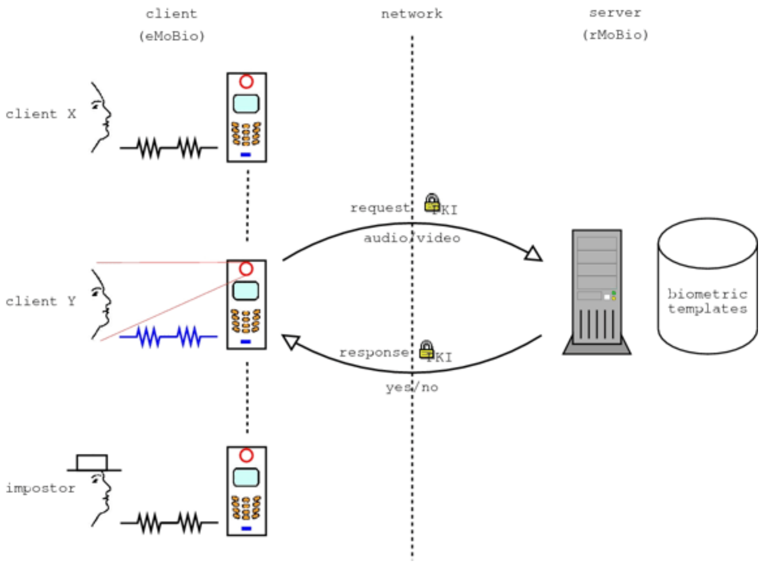


*Figure 4. BioSign client/server architecture.*

## 2.2.Embedded and Scalable Biometry

A scenario where authentication completely takes place on a remote server is not enough for many real life use cases. However, there are considerable challenges that must be overcome for authentication to take place on a mobile device. For this reason MOBIO studies not only offline authentication (on a remote server) but also embedded authentication. This means that there are two main biometry systems which the MOBIO project will examine, these being:

- Embedded biometry (**eMoBio**): In this case the bi-modal biometric authentication technology is embedded on the device and could be used to authenticate its user to allow use of the device. It is running entirely on a portable device and is designed to maximize the authentication performance and to minimize resources such as CPU, memory and speed.
- Remote biometry (**rMoBio**): In this case the bi-modal biometric authentication technology is remote or only partially embedded to access bank account details, micro payments services or other services. If the authentication system needs too many resources to reach the required performance, it will be hosted on a server. Thus, the authentication itself will be done remotely while a minimum of essential functionalities would stay on the client (mobile device) such as data capture, segmentation, preprocessing and feature extraction.

# 3.Current Telecommunication Directions

## 3.1.Introduction

The communication market is evolving rapidly. New players emerge and new application scenarios appears almost daily. As a result new partnerships are being formed and old boundaries for technology and integration fade away.

In this changing environment, operators and integrators explore new revenue ways to reduce operating costs, and provide solutions that increase user confidence and reduce production costs. The successful operator must be able to provide a multitude of new services. Many of these services will be available by both mobile and fixed access with transparent access for the user. Others will represent a combination of TV, Internet and telephony, in the form of converged services.

Technologies that enable converged services exist already. The Internet Protocol (IP) and the Internet paradigm are being introduced in all areas of communication. Rapid development of radio technology leading to increased bit rates (WiMAX being a well-known example). Support for mobility enables truly converged services: this means that the same end-user service can be reached by both mobile and fixed access via the same (or similar) user interface and application architecture.

Operators and integrators that adapt their strategic business plan by considering this changing environment, notably by considering an early introduction of converged services, are expected to gain a competitive edge. Furthermore, the introduction of layered architectures is showing how to improve efficiency, flexibility and enable a smooth introduction of the IMS, a recently introduced milestone for efficient converged service scenarios.

In the next the section current and future directions of mobile telecommunications, in terms of convergence, are described. The current market opportunities for secure mobile services are then outlined.

## 3.2.Convergence and Enabling Technologies

Traditionally, the term fixed-mobile convergence (FMC) has been used by the telecommunication community to identify the integration of landline (fixed) and wireless technologies. However, it now has a broader meaning as convergence also refers to the convergence between media, data communication and telecommunication. This means that a multitude of device-aware services (person to person, person to content and content to person) can be provided to the same user over different access networks and to different device platforms by automatic adaptation of the mobility requirements and quality of service.

The convergence of services implies of course a convergence in devices and networks supporting these services. Common networks already exist supporting several access types, such as WCDMA, GSM, fixed broadband and WLAN. Furthermore, mobile devices support more and more functions in addition to telephony, some examples are cameras, TV, video and email.

When using these services the user expects a similar user interface for most services without having to consider which network or device is used. This means that the services will need to be to be adapted to the device and the access characteristics being used, this includes simplified processes for identification and transactions.

Given the above remarks, it is clear that network and devices must adapt quickly in this dynamic environment. As such, service delivery and terminal platforms that enable fast deployment of new converged service possibilities is a requirement to succeed. One element that is helping to make convergence a reality is the evolution towards one common network, which is IP based.

An IP-based network enables many common functions and also reduces the costs associated with planning and operation. The potential savings for operators and integrators are substantial and is one of the most important elements leading to network convergence. Another aspect which is just as important for convergence in the mobile arena has been the continued development of wireless access.

The development of wireless access has recently reached an important breakpoint. This breakpoint now makes it possible to transfer packet data with high bit rates over a mobile radio interface. This is enabling a new generation of services such as broadband Internet access, Video over IP and IP telephony. These developments provide the starting point for truly converged services, meaning that the same end-user service can be reached via both fixed and mobile devices via the same user interface. Figure 5 shows the capabilities of some radio technologies.

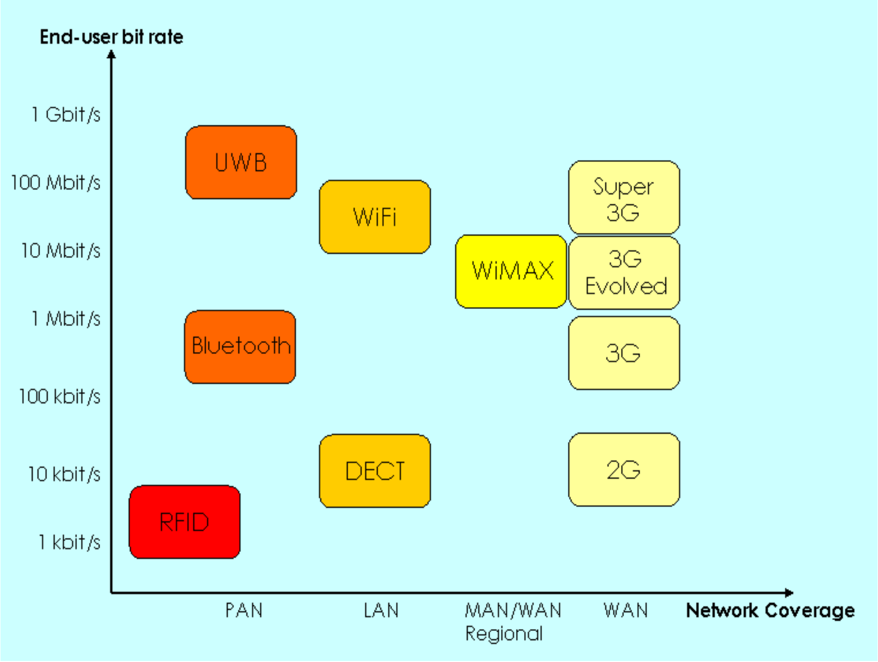


*Figure 5. Radio technology Network Coverages and Bit-rates*

Network operators already offer some convergence which means that user services can be deployed independently of the evolution of networks and devices. This convergence will by helped by new standards that have recently been proposed. Some common technology is at the core of the most recent trend in application and service convergence. An example of current technology helping to provide convergent networks is IMS.

IMS is a standardized solution for Session Initiation Protocol (SIP) based applications for multiple accesses. It is a key component for delivering converged services with the necessary quality of service. IMS makes it possible to increase network efficiency and makes the introduction of new services faster and easier. Also, the common service execution environment of IMS supports user applications that are available over multiple accesses; this is a key element for many converged services. Applications for this technology include active phone books which can be enabled by presence in IMS.

Developed by the 3GPP as a standardized, functional, layered, architecture for cellular next generation networks (NGNs), IMS is now evolving beyond its roots. As well as supporting multiple types of access, such as 3G, WiFi and WiMAX, it also enables operators to deploy multiple quality of service managed applications through a centralized IP session-control, registration and charging platform. Based on SIP, it is well-suited to next-generation session-oriented services like push-to-talk, IM, presence and video, with a potential roadmap towards mobile VoIP and other advanced services.

### Security for IMS platforms

The IMS authentication, authorization and accounting (AAA) server can be used with a Subscriber Identity Module (or SIM card) and operates in environments where the primary subscriber database is a Home Subscriber Server (HSS) which contains the user profile information. The particular AAA protocol used for the IMS service framework is Diameter; this is a recent protocol which replaces the RADIUS protocol and it is defined in IETF RFC 3588 . Diameter security is provided by Internet Protocol Security (IPSEC) or Transport Layer Security (TLS), the latter is already implemented by a number of service providers.

The primary goal of the TLS Protocol is to provide privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. At the lowest level, layered on top of some reliable transport protocol (e.g., TCP), is the TLS Record Protocol which assures that a communication is private and reliable.

The TLS Handshake Protocol provides connection security that has three basic properties:

- The peer's identity can be authenticated using asymmetric, or public key, cryptography
- The negotiation of a shared secret is secure
- The negotiation is reliable: no attacker can modify the negotiation communication without being detected by the parties to the communication.

### Conclusion

Convergence is a ubiquitous trend in market solutions. It is pivotal to offer transparency to the end user in terms of applications and devices. Many tools and terminals exist already for high performance platforms but mobile devices still need considerable research and development to allow the full realization of the IMS and FMC concepts.

## 3.3.Market Opportunities for Secure Mobile Services

The market for secure mobile services is growing substantially. This growth is driven because of interest from the mainstream consumer base. Steve Mansfield, vice president of marketing with AuthenTec, was recently quoted as saying that “... one of the biggest surprises domestic service providers found is that interest in cell phone security is strong among mainstream consumers, not just enterprise accounts. Service providers are starting to give more value-added services. Security issues in cell phones are now becoming a top priority.[1]"

The comments made by Steve Mansfield are supported by a recent scientific survey of more than 2,000 adults sponsored by AuthenTec. This survey showed that 71 percent of the consumers would pay more for a biometric security feature in their cellular phones. In fact it was found that "Most consumers said they would use the technology to replace their PC and Internet passwords, as well as to help transform their cell phones into their personal wallets to conduct m-commerce and wireless banking.[2]"

This survey demonstrates the huge potential in this area. Gary Shapiro, CEO of the Consumer Electronics , was quoted as saying that "The survey shows that biometric sensors are a huge growth area. We are at the infancy of what will be a very large growth curve, heading toward biometric sensing devices becoming an important feature in consumer electronics.[2]"

MOBIO is focused on developing unintrusive mobile biometric technologies using video and voice. The aim is to answer the need for biometric technologies that is already present in the cellphone market; as shown by the introduction of mobile phones with fingerprint sensors. The use of voice and face is considered to be superior to fingerprint as the voice and face are used in natural interaction with the mobile device, for instance when making a video call. Also, the face is already a socially accepted biometric, as is shown by its prevalence in passports and identity cards, and a recent trend report found that voice recognition is a technology that is well accepted by the public[3]. Another advantage of using voice and face based authentication is that it is possible to create a natural interaction with the user.

With voice technology, using speech recognition and voice authentication, it is possible to create interactions with the user. This increases the accuracy and reliability of positively identifying the user while enabling them to navigate help desk and other activities without human intervention. The increased accuracy comes because there are many more samples of the voice and also because it is difficult to use pre-recorded responses to what can be open ended questions. It is foreseen that when face is added to this the complementary information should lead to an even better level of security.

Of course this increased level of security needs to be supported by equivalently secure communication protocols. This is mainly an issue for the service provider offering the MOBIO-enabled services; nevertheless the MOBIO terminal must be able to comply with the requested security features. Targeting applications that implement support for the new IMS framework, this point is well-covered. In particular the integration of MOBIO technology in EPM Communicator suite will offer the support of the TLS protocol mentioned above, which is part of the IMS security layer.

The use of biometric traits such as voice and image can introduce further concerns about privacy of stored data. However, it must be noticed that data on servers will never be picture and voice recordings but non-invertible face and voice features.

[1] http://www.technewsworld.com/story/37600.html?welcome=1209383169

[2] http://biometricwatch.com/BW_in_print/consumer_survey_biometrics.htm

[3] European Biometrics Portal: "Biometrics in Europe". Trend report 2007

# 4.State-of-the-Art in Mobile Devices

## 4.1.Introduction

The development of mobile devices is now being driven by the fundamental principle of convergence. This can be seen by the fact the many available devices already offer to the user several types of connectivity, which must be in most cases manually selected. Also, in the short to medium term it is foreseen that mobile devices will have support for Unlicensed Mobile Access (UMA). This allows a mobile phone to use either WLAN or Bluetooth to access the local fixed broadband to connect to the GSM network. Furthermore, in the future, IP telephony needs to be implemented in the communications protocol of the device so that future convergence opportunities can be fully deployed.

The pace of evolution in this convergence for mobile devices is increasing almost daily, as new access and media technologies are introduced. It can be expected that additional access technologies will lead to extra cost for the device, in addition, storage requirements and capabilities will also greatly increase in both devices and networks.

It must be noticed, as a complementary remark, that some key network characteristics must also be available in devices connected to fixed networks. The evolution of connected home networks with a multitude of applications, such as interactive TV, games, music downloads, shopping and home security, will require some of the characteristics that are delivered by IMS (such as quality of service, user management, charging and security).

## 4.2.Chipsets

State-of-the-art mobile communication devices present a broad range of different specifications and characteristics. Apart from the processor cores, which have converged towards the ARM solution and the same basic instruction set, all the other features vary widely. This has led to a large number of different platforms and solutions.

Many chipsets exist based on different families of ARM cores. TI OMAP, Samsung, Intel, Qualcomm are among the most commonly adopted solutions; it must be noted that the ARM core is characterized by a reduced instruction set, that notably does not provide operations like division or square root nor floating-point formats implemented in hardware. The ARM4/4I Instruction Set is currently the most widespread among existing devices and it only provides fixed-point arithmetic.

Some chipset enhancements targeting multimedia applications are being introduced, such as those in the iPhone chipset. However, there is currently no standard method to add these multimedia enhancements and no clear standard is expected for at least the next few years. Furthermore, even when these complex operation are available they may not be available in terms of development kits; for instance the enhanced features with the support of ARMv6 architecture include advanced SIMD co-processors and a vector floating-point (VFP) co-processor but there is no real evidence of ARMv6 support in a software development kit.

## 4.3.Operating Systems

There are several operating systems created specifically for mobile devices, these include Symbian, Windows Mobile and embedded Linux. In terms of sold copies, Symbian is the most widely adopted mobile operating system (OS), however, the Symbian OS is a particularly difficult environment to perform research and development. Therefore, the other widespread operating systems, Windows Mobile and embedded Linux, seem to be better candidates for a project like MOBIO. Given EyePMedia's experience in development on the Windows Mobile OS this is the preferred operating system for this project.

## 4.4.Requirements and Constraints

The MOBIO project requires mobile devices which have:

- a standard mobile-device quality microphone, with the possibility to connect a hands-free set. For acquisition of MOBIO database and experimenting, it would be optimal to be able to record from both microphones simultaneously (but this is normally switched in hardware at connection, as far as it is known)
- a frontal camera (typically available for 3G devices) with good quality and ideally able to capture video at 15 frames per second (fps)
- audio and video that can be captured simultaneously to guarantee synchronization of both streams
- a Wi-Fi connection to transfer captured data over wider band radio instead of the GPRS network

These requirements need to take into consideration that the MOBIO project will have severe limitations. These limitations are because of the capabilities of currently available mobile devices, and even with the next generation of mobile devices. These limitations include:

- low quality video capture: the VGA format is hardly usable without hardware accelerators, as a consequence it is more likely that the video will be captured as QVGA ideally at 15 fps
- fixed-point format in most of the processing operations
- reduced memory (a few tens of MBytes) and processing resources (less than 1 GHz processors)
- a Software Development Environment with reduced functionality in comparison to most desktop and workstation platforms

## 4.5.State-of-the-Art Devices

There are many state-of-the-art mobile devices that need to be considered. A summary of the candidate devices is presented in the following tables. The devices presented are not representative of market shares but instead focus on new or announced devices that correspond to possible development candidates. At a first glance many devices offer similar functionality and this may be true from the user point of view. In fact, it is fundamental for a research project such as MOBIO to pay attention to the available development resources. For instance, almost all of the reviewed devices have advanced technological aspects which cannot be used for development, this is due to a lack of appropriate Software Development tools.

# Apple iPhone 16GB Specifications

| | |
|---|---|
| **Datasheet State:** | **Final specifications** |
| **Release Date:** | February, 2008 |
| **Dimensions:** | 61 x 115 x 11.6 millimetres |

## Software Environment

| | |
|---|---|
| **Operating System:** | Apple Mac OS X v1.0 (ARM) |

## Microprocessor

| | |
|---|---|
| **CPU:** | 32bit Samsung S5L8900 (Chipset) |
| **CPU Clock:** | 620 MHz |

## Memory, Storage capacity

| | |
|---|---|
| **ROM capacity:** | 16000 MB |
| **RAM capacity:** | 128 MB |
| **Hard Disk capacity:** | Not supported |

## Display

| | |
|---|---|
| **Display Type:** | color transflective TFT , 65536 scales |
| **Display Resolution:** | 320 x 480 |
| **Display Diagonal:** | 3.5 " |

## Sound

| | |
|---|---|
| **Microphone:** | mono |
| **Speaker:** | mono |
| **Audio Output:** | 3.5mm plug |

## Cellular Phone

| | |
|---|---|
| **Cellular Networks:** | GSM850, GSM900, GSM1800, GSM1900 |
| **Cellular Data Link:** | CSD, GPRS, EDGE |
| **Call Alert:** | 64 -chord melody |
| **Vibrating Alert:** | Supported |

## Control Peripherals

| | |
|---|---|
| **Positioning Device:** | Multi-touch screen |

| | |
|---|---|
| **Primary Keyboard:** | Not supported |
| **Directional Pad:** | Not supported |
| **Scroll Wheel:** | Not supported |

## Interfaces

| | |
|---|---|
| **Expansion Slots:** | Not supported |
| **USB:** | USB 2.0 client, Full-Speed (12Mbit/s)<br>USB Series Mini-B (mini-USB) connector |
| **Infrared Gate:** | Not supported |
| **Bluetooth:** | Bluetooth 2.0 + EDR |
| **Wireless LAN:** | 802.11b, 802.11g |

## Multimedia Telecommunication

| | |
|---|---|
| **Analog TV:** | Not supported |
| **Analog Radio:** | Not supported |

## Built-in Digital Camera

| | |
|---|---|
| **Main Camera:** | CMOS sensor, 1.9MP (rear camera) |
| **Optical Zoom:** | 1 x |
| **Built-in Flash:** | Not supported |

## Power Supply

| | |
|---|---|
| **Battery:** | Lithium-ion , built-in |

# Meizu M8 miniOne Specifications

| | |
|---|---|
| **Datasheet State:** | **Preliminary specifications** |
| **Release Date:** | April, 2008 |
| **Dimensions:** | 59 x 107 x 11.8 millimetres |

## Software Environment

| | |
|---|---|
| **Operating System:** | Microsoft Windows CE 6.0 Core (Yamazaki) miniOne GUI |

## Microprocessor

| | |
|---|---|
| **CPU:** | 32bit Samsung S5L8900 (Chipset) |
| **CPU Clock:** | 667 MHz |

## Memory, Storage capacity

| | |
|---|---|
| **ROM capacity:** | 8192 MB |
| **RAM capacity:** | 128 MB |
| **Hard Disk capacity:** | Not supported |

## Display

| | |
|---|---|
| **Display Type:** | color transflective TFT , 16777216 scales |
| **Display Resolution:** | 480 x 720 |
| **Display Diagonal:** | 3.3 " |

## Sound

| | |
|---|---|
| **Microphone:** | mono |
| **Speaker:** | stereo |
| **Audio Output:** | 2.5mm plug |

## Cellular Phone

| | |
|---|---|
| **Cellular Networks:** | GSM900, GSM1800, GSM1900 |
| **Cellular Data Link:** | CSD, GPRS, EDGE |
| **Call Alert:** | 64 -chord melody |
| **Vibrating Alert:** | Supported |

## Interfaces

| | |
|---|---|
| **Expansion Slots:** | MMC, SD, SDHC, SDIO |

| | |
|---|---|
| **USB:** | USB 2.0 host/client, Hi-Speed (480Mbit/s), OTG 1.2 compliant<br>USB Series Mini-B (mini-USB) connector |
| **Infrared Gate:** | Not supported |
| **Bluetooth:** | Bluetooth 2.0 + EDR |
| **Wireless LAN:** | 802.11b, 802.11g |

## Built-in Digital Camera

| | |
|---|---|
| **Main Camera:** | CMOS sensor, 3.1MP (rear camera) |
| **Autofocus (AF):** | Supported |
| **Optical Zoom:** | 1 x |
| **Built-in Flash:** | Not supported |
| **Secondary Camera:** | CMOS sensor, 640x480 pixel (frontal camera) |

## Power Supply

| | |
|---|---|
| **Battery:** | Lithium-ion , removable |
| **Battery Capacity:** | 1400 mAh |

# HTC S730 US (HTC Wings 200) Specifications

| | |
|---|---|
| **Datasheet State:** | **Final specifications** |
| **Release Date:** | February, 2008 |
| **Dimensions:** | 51 x 105.8 x 19.4 millimetres |
| **Mass:** | 150 grams (battery included) |

## Software Environment

| | |
|---|---|
| **Operating System:** | Microsoft Windows Mobile 6 Standard (Crossbow) |

## Microprocessor

| | |
|---|---|
| **CPU:** | 32bit Qualcomm MSM7200 (Chipset) |
| **CPU Clock:** | 400 MHz |

## Memory, Storage capacity

| | |
|---|---|
| **ROM capacity:** | 256 MB |
| **RAM capacity:** | 64 MB |
| **Hard Disk capacity:** | Not supported |

## Display

| | |
|---|---|
| **Display Type:** | color transflective TFT , 65536 scales |
| **Display Resolution:** | 240 x 320 |
| **Display Diagonal:** | 2.4 " |

## Sound

| | |
|---|---|
| **Microphone:** | mono (bottom) |
| **Speaker:** | mono |
| **Audio Output:** | Proprietary plug |

## Cellular Phone

| | |
|---|---|
| **Cellular Networks:** | GSM850, GSM900, GSM1800, GSM1900, UMTS850, UMTS1900, UMTS2100 |
| **Cellular Data Link:** | CSD, GPRS, EDGE, UMTS, HSDPA |
| **Call Alert:** | 40 -chord melody |
| **Vibrating Alert:** | Supported |

## Control Peripherals

| | |
|---|---|
| **Positioning Device:** | Not supported |
| **Primary Keyboard:** | Slide-out QWERTY-type keyboard, 31 keys |
| **Secondary Keyboard:** | Built-in numeric phone keyboard, 22 keys |
| **Directional Pad:** | 5 -way block |
| **Scroll Wheel:** | Not supported |

## Interfaces

| | |
|---|---|
| **Expansion Slots:** | microSD, microSDHC, TransFlash, SDIO |
| **USB:** | USB 2.0 client, Full-Speed (12Mbit/s)<br>USB Series Mini-B (mini-USB) connector |
| **Infrared Gate:** | Not supported |
| **Bluetooth:** | Bluetooth 2.0 |
| **Wireless LAN:** | 802.11b, 802.11g |

## Built-in Digital Camera

| | |
|---|---|
| **Main Camera:** | CMOS sensor, 1.9MP (rear camera) |
| **Optical Zoom:** | 1 x |
| **Built-in Flash:** | Not supported |
| **Secondary Camera:** | CMOS sensor, 640x480 pixel (frontal camera) |

## Power Supply

| | |
|---|---|
| **Battery:** | Lithium-ion polymer , removable |
| **Battery Capacity:** | 1050 mAh |

## Toshiba Portégé G810 Specifications

| | |
|---|---|
| **Datasheet State:** | **Final specifications** |
| **Release Date:** | May, 2008 |
| **Dimensions:** | 58 x 110 x 14 millimetres |
| **Mass:** | 120 grams (battery included) |

### Software Environment

| | |
|---|---|
| **Operating System:** | Microsoft Windows Mobile 6 Professional (Crossbow) |

### Microprocessor

| | |
|---|---|
| **CPU:** | 32bit Qualcomm MSM7200 |
| **CPU Clock:** | 400 MHz |

### Memory, Storage capacity

| | |
|---|---|
| **ROM capacity:** | 256 MB |
| **RAM capacity:** | 128 MB |
| **Hard Disk capacity:** | Not supported |

### Display

| | |
|---|---|
| **Display Type:** | color transflective TFT , 65536 scales |
| **Display Resolution:** | 240 x 320 |
| **Display Diagonal:** | 2.8 " |

### Sound

| | |
|---|---|
| **Microphone:** | mono |
| **Speaker:** | stereo |
| **Audio Output:** | 2.5mm plug |

### Cellular Phone

| | |
|---|---|
| **Cellular Networks:** | GSM850, GSM900, GSM1800, GSM1900, UMTS850, UMTS1900, UMTS2100 |
| **Cellular Data Link:** | CSD, GPRS, EDGE, UMTS, HSDPA, HSUPA |
| **Call Alert:** | 40 -chord melody |
| **Vibrating Alert:** | Supported |

### Control Peripherals

| | |
|---|---|
| **Positioning Device:** | Touchscreen |
| **Primary Keyboard:** | Not supported |
| **Directional Pad:** | 5 -way block |
| **Scroll Wheel:** | Not supported |

### Interfaces

| | |
|---|---|
| **Expansion Slots:** | microSD, microSDHC, TransFlash, SDIO |
| **USB:** | USB 2.0 client, Full-Speed (12Mbit/s)<br>USB Series Mini-B (mini-USB) connector |
| **Infrared Gate:** | Not supported |
| **Bluetooth:** | Bluetooth 2.0 + EDR |
| **Wireless LAN:** | 802.11b, 802.11g |

### Multimedia Telecommunication

| | |
|---|---|
| **Analog TV:** | Not supported |
| **Analog Radio:** | FM radio receiver |

### Satellite Navigation

| | |
|---|---|
| **Built-in GPS:** | NMEA 0183 |

### Built-in Digital Camera

| | |
|---|---|
| **Main Camera:** | CMOS sensor, 2.8MP (rear camera) |
| **Optical Zoom:** | 1 x |
| **Built-in Flash:** | Mobile light (LED) |
| **Secondary Camera:** | CMOS sensor, 640x480 pixel (frontal camera) |

### Power Supply

| | |
|---|---|
| **Battery:** | Lithium-ion , removable |
| **Battery Capacity:** | 1530 mAh |

# LG KS20 Specifications

| | |
|---|---|
| **Datasheet State:** | **Final specifications** |
| **Release Date:** | November, 2007 |
| **Dimensions:** | 58 x 99.8 x 12.8 millimetres |
| **Mass:** | 92.5 grams (battery included) |

## Software Environment

| | |
|---|---|
| **Operating System:** | Microsoft Windows Mobile 6 Professional (Crossbow) AKU 0.4.5 |

## Microprocessor

| | |
|---|---|
| **CPU:** | 32bit Qualcomm MSM7200 (Chipset) |
| **CPU Clock:** | 400 MHz |

## Memory, Storage capacity

| | |
|---|---|
| **ROM capacity:** | 256 MB (accessible: 148.85MB) |
| **RAM capacity:** | 128 MB (accessible: 80.75MB) |
| **Hard Disk capacity:** | Not supported |

## Display

| | |
|---|---|
| **Display Type:** | color transflective TFT , 262144 scales |
| **Display Resolution:** | 240 x 320 |
| **Display Diagonal:** | 2.8 " |

## Sound

| | |
|---|---|
| **Microphone:** | mono |
| **Speaker:** | mono |

## Cellular Phone

| | |
|---|---|
| **Cellular Networks:** | GSM900, GSM1800, GSM1900, UMTS2100 |
| **Cellular Data Link:** | CSD, GPRS, EDGE, UMTS, HSDPA |
| **Call Alert:** | 72 -chord melody |
| **Vibrating Alert:** | Supported |

## Control Peripherals

| | |
|---|---|
| **Positioning Device:** | Touchscreen |

| | |
|---|---|
| **Primary Keyboard:** | Not supported |
| **Directional Pad:** | 5 -way block |

## Interfaces

| | |
|---|---|
| **Expansion Slots:** | microSD, TransFlash, SDIO |
| **USB:** | USB 2.0 client, Full-Speed (12Mbit/s)<br>USB Series Mini-B (mini-USB) connector |
| **Infrared Gate:** | Not supported |
| **Bluetooth:** | Bluetooth 2.0 |
| **Wireless LAN:** | 802.11b, 802.11g |

## Built-in Digital Camera

| | |
|---|---|
| **Main Camera:** | CMOS sensor, 1.9MP (rear camera) |
| **Autofocus (AF):** | Supported |
| **Optical Zoom:** | 1 x |
| **Built-in Flash:** | Mobile light (LED) |
| **Secondary Camera:** | CMOS sensor, 640x480 pixel (frontal camera) |

## Power Supply

| | |
|---|---|
| **Battery:** | Lithium-ion polymer , removable |
| **Battery Capacity:** | 1050 mAh |

# Asus M536 Specifications

| | |
|---|---|
| **Datasheet State:** | **Preliminary specifications** |
| **Release Date:** | May, 2008 |
| **Dimensions:** | 62.5 x 116.9 x 13.9 millimetres |

## Software Environment

| | |
|---|---|
| **Operating System:** | Microsoft Windows Mobile 6 Professional (Crossbow) |

## Microprocessor

| | |
|---|---|
| **CPU:** | 32bit Texas Instruments OMAP 2430 |
| **CPU Clock:** | 400 MHz |

## Memory, Storage capacity

| | |
|---|---|
| **ROM capacity:** | 256 MB |
| **RAM capacity:** | 128 MB |
| **Hard Disk capacity:** | Not supported |

## Display

| | |
|---|---|
| **Display Type:** | color transflective TFT , 65536 scales |
| **Display Resolution:** | 320 x 320 |
| **Display Diagonal:** | 2.4 " |

## Sound

| | |
|---|---|
| **Microphone:** | mono |
| **Speaker:** | mono |
| **Audio Output:** | 2.5mm plug |

## Cellular Phone

| | |
|---|---|
| **Cellular Networks:** | GSM900, GSM1800, GSM1900, UMTS850, UMTS1900, UMTS2100 |
| **Cellular Data Link:** | CSD, GPRS, EDGE, UMTS, HSDPA |
| **Call Alert:** | 40 -chord melody |
| **Vibrating Alert:** | Supported |

## Control Peripherals

| | |
|---|---|
| **Positioning Device:** | Touchscreen |
| **Primary Keyboard:** | Built-in QWERTY-type keyboard, 37 keys |
| **Directional Pad:** | 4 -way block |

## Interfaces

| | |
|---|---|
| **Expansion Slots:** | microSD, microSDHC, TransFlash, SDIO |
| **USB:** | USB 1.1 client, Full-Speed (12Mbit/s)<br>USB Series Mini-B (mini-USB) connector |
| **Infrared Gate:** | Not supported |
| **Bluetooth:** | Bluetooth 2.0 + EDR |
| **Wireless LAN:** | 802.11b, 802.11g |

## Satellite Navigation

| | |
|---|---|
| **Built-in GPS:** | NMEA 0183 |

## Built-in Digital Camera

| | |
|---|---|
| **Main Camera:** | CMOS sensor, 3.1MP (rear camera) |
| **Autofocus (AF):** | Supported |
| **Optical Zoom:** | 1 x |
| **Secondary Camera:** | CMOS sensor, 640x480 pixel (frontal camera) |

## Power Supply

| | |
|---|---|
| **Battery:** | Lithium-ion , removable |
| **Battery Capacity:** | 1200 mAh |

# NOKIA N96 Specifications

| | |
|---|---|
| **Datasheet State:** | **Preliminary specifications** |
| **Release Date:** | July, 2008 |
| **Dimensions:** | 55 x 103 x 18 millimetres |

## Software Environment

| | |
|---|---|
| **Operating System:** | Symbian OS 9.2 Series 60 3rd Edition 3.1 Feature Pack 2 |

## Microprocessor

| | |
|---|---|
| **CPU:** | 32bit ST Microelectronics Nomadik STn8816 |
| **CPU Clock:** | 334 MHz |

## Memory, Storage capacity

| | |
|---|---|
| **ROM capacity:** | 16640 MB (accessible: 16560MB) |
| **RAM capacity:** | 128 MB |
| **Hard Disk capacity:** | Not supported |

## Display

| | |
|---|---|
| **Display Type:** | color transflective TFT , 16777216 scales |
| **Display Resolution:** | 240 x 320 |
| **Display Diagonal:** | 2.8 " |

## Sound

| | |
|---|---|
| **Microphone:** | mono |
| **Speaker:** | stereo |
| **Audio Output:** | 3.5mm plug |

## Cellular Phone

| | |
|---|---|
| **Cellular Networks:** | GSM850, GSM900, GSM1800, GSM1900, UMTS900, UMTS2100 |
| **Cellular Data Link:** | CSD, HSCSD, GPRS, EDGE, UMTS, HSDPA |
| **Call Alert:** | 64 -chord melody |
| **Vibrating Alert:** | Supported |

## Control Peripherals

| | |
|---|---|
| **Positioning Device:** | Touchpad |

| | |
|---|---|
| **Primary Keyboard:** | Slide-out numeric phone keyboard, 12 keys |
| **Directional Pad:** | 4 -way block |
| **Scroll Wheel:** | Not supported |

## Interfaces

| | |
|---|---|
| **Expansion Slots:** | microSD, microSDHC, TransFlash, SDIO |
| **USB:** | USB 2.0 client, Hi-Speed (480Mbit/s)<br>USB Series Micro-B (micro-USB) connector |
| **Infrared Gate:** | Not supported |
| **Bluetooth:** | Bluetooth 2.0 + EDR |
| **Wireless LAN:** | 802.11b, 802.11g |

## Multimedia Telecommunication

| | |
|---|---|
| **Analog TV:** | Not supported |
| **Analog Radio:** | FM radio receiver |
| **Digital Media Broadcast:** | DVB-H tuner |

## Satellite Navigation

| | |
|---|---|
| **Built-in GPS:** | NMEA 0183 |

## Built-in Digital Camera

| | |
|---|---|
| **Main Camera:** | CMOS sensor, 5MP (rear camera) |
| **Autofocus (AF):** | Supported |
| **Macro Mode:** | Supported |
| **Built-in Flash:** | Mobile light (LED) |
| **Secondary Camera:** | CMOS sensor, 640x480 pixel (frontal camera) |

## Power Supply

| | |
|---|---|
| **Battery:** | Lithium-ion , removable |
| **Battery Capacity:** | 950 mAh |

## 4.6.Device Summary Table

| Device | Microphone | Frontal Camera | WiFi | RAM Memory | CPU Clock | Availability |
|---|---|---|---|---|---|---|
| iPhone | *mono* | *no* | *yes* | *128 Mb* | *620 MHz* | *yes* |
| Meizu M8 | *mono* | *yes* | *yes* | *128 Mb* | *667 MHz* | *Aug 08* |
| HTC S730 | *mono* | *yes* | *yes* | *64 Mb* | *400 MHz* | *yes* |
| G810 | *mono* | *yes* | *yes* | *128 Mb* | *400 MHz* | *yes* |
| LG KS20 | *mono* | *yes* | *yes* | *80 Mb* | *400 MHz* | *yes* |
| Asus M536 | *mono* | *yes* | *yes* | *128 Mb* | *400 MHz* | *July 08* |
| Nokia N96 | *mono* | *yes* | *yes* | *128 Mb* | *334 MHz* | *Oct 08 (N95 yes)* |

# 5.Use Case Scenarios

This section describes five use cases for the MOBIO biometric-enabled authentication technology. The specification of these use cases was conceived with several of EyePMedia's integrated tools in mind; such as VoIP softphones with forthcoming FMC support. Still, most of the use cases are self-standing even without these tools.

The purpose of the use cases is to detail the conditions and scenarios in order to facilitate the specification of the MOBIO database and protocols (see Deliverable 2.2). However, the conditions and scenarios still need to cover actual market and user needs and to also take into account the constraints and requirements emerging from the previous sections on biometric-enabled communication applications, telecommunication systems (convergence) and analysis of mobile devices. It's noted that the effect of these elements have been projected as far as possible over a three years span so that they can be achieved within the time frame of the MOBIO project.

## 5.1.Description of Use Case Scenarios

The are numerous use case scenarios that MOBIO could address but to have a realistic goal the number of use case scenarios considered in the MOBIO project is reduced to five. The five use cases were chosen to describe the broad range of contributions that mobile biometry can make. These five use cases range from assisting people in performing bank orders through to matching their biometric features against those of their friends or movie stars. The use cases are described in detail below.

### Bank Order

In this use case it is envisaged that a customer of a bank places an order by phone using a video call. This use case presents a high security scenario with a great potential market (if successful). Current voice only identification applications have enormous error rates and the current solutions, which are based on private questions or codes, are not perceived as “very” secure by customers and operators. It is noted that it may be hard to obtain the necessary level of security to achieve a successful impact on the market.

| | |
|---|---|
| UCId | UC001 |
| Use case | Bank Order |
| Description | A Customer of a bank places an order by phone via an audio/video call. |
| Actors | - Customer (C)<br>- Bank employee (B) |
| Assumptions | Customer model of C already collected and stored in the Bank System (BS).<br>Collection of the customer models has been done by a local session at a bank agency by trusted and trained personnel. Session time is in the order of a few to ten minutes maximum in the case that no |

| | |
|---|---|
| | problems occur (which means that the collected data is valid most of the time), otherwise some extra time may be allowed.<br>Registration can be made remotely, assuming that this takes place by certified terminals and a secure network (it is up to the bank to provide this technology if requested).<br>Sessions are recorded in compressed format for both audio and video, with formats similar to those used for customer calls: audio will be narrow-band (8 kHz, 16-bit) and video will be h264 CIF format at 10 or 15 fps.<br>Customer calls are done either by softphones (EPM or other) or possibly by hardware tools (a normal mobile or fixed phone); the customer is aware that a lower quality device may lower the probability of a successful transaction (success rates will be established based on EPM softphones).<br>The authentication system provides a score to be used by B to proceed further (final decision is up to B). |
| Steps | 1. C calls B using his/her video cell phone through a bi-modal call.<br>2. B answers the call (by desktop or mobile client), and starts the research of the claimed identity on the BS database. The profile is found quickly.<br>3. C indicates his/her wish to make a transaction T.<br>4. B asks a small number of questions to C (see Dialog Manager in Deliverable 2.2) possibly related to the transaction (account number or the type of transactions) but with the non-hidden purpose of having a first authentication score on C. C is informed that this call may be recorded (remotely, configurable audio-only or audiovisual this is up to the bank to choose).<br>5. While asking questions or getting answers, the BS provides the Authentication level in percentage.<br>6. C is the real customer; after a number of answers, the percentage score must be above a level X (say 99%) allowing B to proceed with the real transaction detail in good security.<br>7. While the transaction proceeds, with the discussion of details, authentication is continuing to be refined.<br>8. At a certain point, near the end of the transaction (typically 30-60 seconds), ~certitude (no false positive admitted, or 99.99%) is reached and the transaction can be finalized (the data is confirmed in the transaction procedure and the transaction is registered).<br>9. The call ends. |
| Post-Conditions | Both parts receive by email a call ID notification.<br>Customer may be further requested to reply to this email. |
| Variations | ● At step 2, for an increased level of security, B calls back A on a trusted agreed number instead of answering the call.<br>● C is not the real customer, but has a similar face and voice. In this case, the Authentication Level should be inferior to |

| | |
|---|---|
| | level Y (say 25%). Below this level transaction will be refused.<br>● C is the real customer, but using only audio call. In this case, the Authentication Level should be superior to level Z (say 95%) to start the transaction. A more limited set of transactions will be possible in this mode, and it can be finalized with an authentication score of at least 99%.<br>● C is not the real customer, but has a similar voice and uses audio only. Same constraints as above for the transaction but in this case the Authentication Level should be inferior to level W (say 35%). |
| Asynchronous Actions | The Customer may be requested to change his/her setup or environmental conditions during the transaction because authentication is not positive enough. The customer can change setup or conditions **during** the call and authentication should continue from previously captured data when possible. |
| Issues | Hardware telephones with good network conditions must guarantee the same success ratio of soft-phones.<br>A certain amount of false negatives can be admitted (1 %, i.e. 1 time out of 100 a positive falls below 99), for which customer C may be requested to call again in different conditions (telephone, webcam or in a private room) instead of going on as above.<br>Enrolling conditions are somehow different than call conditions.<br>Accuracy in security is required. |
| Trust and Threat Issues | ● Data Confidentiality. No confidential information is transmitted except in case of remote enrollment. Data (customer models) are stored uniquely on the bank server, they are not transmitted at every call. It may be possible to pre-process streams and transmit some partial processing results with the call (for instance bounding boxes ) but this does not reveal useful information that could be use to reverse engineer the authentication algorithm or to interfere with the authentication process.<br>● Data Integrity. The use of TLS (see section 3.2 above) in an IMS framework, with possible authentication in both directions, guarantees an excellent level of integrity without corruption.<br>● Data Availability. Within the agreed limits of the proposed kind of service, audiovisual call through IP provide a better quality of service (faster authentication, etc.). The requirement of a service possible even in case of simple phone call (hardware telephone) guarantees a worst case solution in case of IP failure. |
| Functional Requirements | Dialog manager<br>Enrollment control at the bank<br>Test conditions uncontrolled (mobile maybe just avoid very critical environments) |

## Trusted peer-to-peer video-chat

In this use case it is envisaged that two people are having an audio-video meeting possibly using their mobile phone and that an online service is used to ensure some level of security for the meeting. This is a low security scenario as no money risk is involved in this use case, however, because it is a chat scenario there are some possible privacy issues. This use case can be seen as a case of Bio-Metric Enabled Public Key.

| UCId | UC002 |
|---|---|
| Use case | Trusted Chat |
| Description | Two people having a video chat from their mobile systems (in hotel room or other similar place), through an online service for virtual meetings. |
| Actors | - User A (A)<br>- User B (B) |
| Assumptions | User model of B is already available (downloaded) on the system of user A (AS) or via a remote server. It might be downloaded at point 3 below.<br>User models are collected in a trusted manner when the user registers to the chat service; for example he receives a password upon payment and he can use this password to connect to the service site and interact with the system to record the user model. He/she may be requested to repeat the procedure if not successful but the session should be rather short, a few minutes maximum; an automated system may drive the user through some predefined conversation.<br>User model recording can take place only by the EPM-based softphone package that will be distributed by the service provider; this also guarantees that sessions can be recorded in compressed format for both audio and video, with formats similar to those used by user calls: audio is narrow- or wide-band (8 kHz or 16 kHz, 16-bit) and video is h264 CIF format at 10 or 15 fps. |
| Steps | 1. B wants to have a video chat with A with his/her desktop system (using a service like MSN, as an example) using EPM software package.<br>2. A receives a chat invitation from B.<br>3. A accepts the invitation, the A toolset downloads or searches for the user model of B. The user model is found. User models may be signed (e.g. by a trusting authority) to improve security of the system.<br>4. A receives audio/video stream from B and starts the on-the-fly authentication process on AS; authentication process is transparent to A and B (as B is also authenticating A) but it might be helped by typical startup conversation (as done by the automated system upon registration); they are of course aware of this as they have the same system.<br>5. A and B start chatting.<br>6. While chatting, AS processes the video/audio stream from B |

| | |
|---|---|
| | and provides in real time the authentication level in percentage to A. They are mapped into 5 levels, with level “Trusted” when above 90%.<br>7. The chat is terminated. |
| Post-Conditions | Negative authentications are recorded and a user may be requested to repeat registration. |
| Variations | ● B is not the real person B, but has a similar face and voice. In this case, the Authentication Level should be inferior to level Y (say 15%).<br>● B is the real user B, but using only audio call (still by EPM toolset). In this case, the authentication level should be superior to level Z (say 70%), corresponding to Level 4.<br>● B is not the real user B, but has a voice and use audio only. In this case, the Authentication Level should be inferior to level W (say 35%). |
| Asynchronous Actions | A sudden visual connection/disconnection may happen, with authentication process adapting since previous conditions. |
| Issues | Recording should not be allowed.<br>Simultaneous users; the background environment is not controllable, many different conversation moods can be imagined. |
| Trust and Threat Issues | ● Data Confidentiality. No confidential information is transmitted except at the moment of remote enrollment. Passwords used for enrollment can be made usable only once to reinforce this point. A notification is sent if the password is used more than once. It may be possible to pre-process streams and transmit some partial processing results with the call (for instance bounding boxes) but this does not reveal useful information and so no reversing of the authentication algorithm is possible. Parts of the authentication algorithm are present on the client tool, but only a highly skilled reverse engineer could use this to interfere with the authentication process.<br>● Data Integrity. The use of TLS (see section 3.2 above) in an IMS framework, with possible authentication in both directions, guarantees an excellent level of integrity without corruption of private conversations<br>● Data Availability. Within the agreed limits of the proposed kind of service, audiovisual call through IP provide a sufficient quality of service. There are no particular urgency constraints in this scenario. |
| Requirements | Enrollment from desktop platform, possibly uncontrolled.<br>Test uncontrolled (mobile and/or desktop). |

## Mobile to Mobile Authentication

In this use case it is necessary to recognize users calling from a reduced set of self-stored users. An example scenario is a parent calling a school to inform them that somebody else is going to pick up their child. In this situation the teacher needs to be sure the person calling is definitely the parent and not somebody else. No server is involved and the scenario is completely local. There is no money risk is involved but there is a high degree of human risk. Reducing the number of acceptable peers (limiting the number of parents enrolled on one phone) can be seen as a counterbalance to the fact that the verification (and enrollment) is on a mobile device.

| UCId | UC003 |
|---|---|
| Use case | Mobile to Mobile Authentication |
| Description | Verification of the identity of a person making a multi-modal call (scenario with limited number of target users and no server available). |
| Actors | - Teacher in a kindergarten (T)<br>- Parent (P) |
| Assumptions | P might need to call the kindergarten and T needs to be sure about the identity of P. One case would be that P needs to inform T that another person will pick up the child. T can be new or from a different class-room and thus does not necessarily know P personally.<br>T can move around the school or be with the kids outside, he/she will have a teacher's mobile device (TMD) on her all the time. She normally has no access to a PC during work with children, so no server solution is possible.<br>In the enrollment phase, P has made a multi-modal call from his/her mobile to TMD. The call is stored and processed by TMD to obtain P's model. The number of targets is limited to several tens.<br>When P makes a call to TMD, he/she is motivated to have his/her identity checked without problems, so P finds a quiet place (P is aware of this constraint). To summarize:<br>● Enrollment phase: P places a call to TMD in the kindergarten under controlled conditions (e.g. child subscription). TMD processes his/her call and creates P's model.<br>● TMD can be transferred to other member of personnel (teachers taking shifts, replacement teachers). There will be one TMD per class-room. |
| Steps | 1. P calls T on her TMD with a request involving security of his/her child. P is aware that his/her identity will be checked during the call.<br>2. T holds a conversation with P, asking for details about P's child or the request.<br>3. During the call, the identity of P is evaluated on TMD (there is a need for light-weight processing, as TMD has limited computing power).<br>4. TMD provides to the teacher authentication level in real time, with a confidence interval, with the level “Trusted” when the level exceeds 90% and the confidence interval is less than 10%. |

| | |
|---|---|
| | 5. In case the authentication level does not reach 90% by the end of call, T can require further authentication, ask P to move to more  suitable environment, or refuse the request.<br>6. The call is ended. |
| Post-Conditions | At the end of the day, T connects the TMD to a PC (together with charging it), calls (if any) are downloaded and processed by more precise algorithms running on PC overnight. A report consisting of<br>● identity of parent<br>● length of call<br>● result of authentication on TMD<br>● result of authentication on a PC<br>is sent to T and to the manager of kindergarten.<br>In the case where authentication is borderline or an impostor attack is suspected it may be possible to upload the data (just after the phone call) to a server PC to perform a more accurate authentication of the person before they arrive.<br>This is also useful to avoid dangerous overflow situations if several calls are received during the same day. |
| Variations | P might use voice only. In this case, T obligatorily asks further authentication data. |
| Asynchronous Actions | In case the authentication level is low for a considerable time, T can secretly call the child concerned to listen to the ongoing conversation and tell whether this is really P.<br>When possible (e.g. inside the school) immediate upload to a server PC for a more precise authentication will be done. |
| Issues | TMD is less powerful than a PC, note that this scenario is without any server. The authentication algorithms will have to be more *lightweight* and therefore less precise. |
| Trust and Threat Issues | ● Data Confidentiality. No confidential information is transmitted except at the moment of enrollment, but this is in protected conditions. The algorithm is present on the client tool but only a highly skilled reverse engineer could use this to interfere with the authentication process (for instance in case the device is stolen). Stored data consists only of user models and not of conversations. Furthermore they can be encrypted in the device.<br>● Data Integrity. The use of TLS (see section 3.2 above) guarantees the level of integrity especially in the enrollment phase. The following calls should not contain a level of information with particular requirements once the remote speaker can be authenticated.<br>● Data Availability. Within the agreed limits of the proposed kind of service, audiovisual call through IP provide a sufficient quality of service. |
| Requirements | Standard mobile capable of multimodal calls on the side of P.<br>More powerful device used as TMD.<br>Verification on the mobile, enrollment from device too |

## Information Retrieval System

This use case shows how it could be possible to retrieve important information remotely. Examples of this use case include contacting a system administrator by a secure means to have a password reset through to retrieving bank account information and results from medical tests (for instance when it is very difficult for someone to leave home due to illness or disease). It is a server-based scenario that does have a high risk factor, however, this can be eased by a more strict enrollment procedure, especially for professional domains.

| UCId | UC004 |
|---|---|
| Use case | Information Retrieval System |
| Description | A user can contact a professional service provider to retrieve personal information concerning such as passwords, keys, bank account information, medical analysis. This scenario is best used for fast retrieval in mobility (or lack of mobility) situations. |
| Actors | - User A (A)<br>- Professional Service (PS) |
| Assumptions | Customer model of A already collected and stored at the Professional Service (PS): bank, insurance agency or hospital.<br>Collection of the customer models has been done by a local session at PS by trusted and trained personnel. Session time is in the order of a few to ten minutes.<br>Registration can be made remotely, assuming that this takes place by certified terminals and secured network (certified offices or medical studios).<br>Requests are possibly transmitted by MMS messages containing user request and authentication information.<br>Customer calls are done either by softphones (EPM or other) or possibly by hardware tools (a normal mobile or fixed phone) able to generate adequate authentication information.<br>The authentication system provides a score to be used by PS to proceed further (final decision is up to PS). |
| Steps | 1. User A needs to recover varying access information (password, key) to a service PS. Only a public desktop wide-band (Internet point) access is available.<br>2. In a private quiet location A composes a multimedia message containing a request and authenticates at the device (a special media type is attached).<br>3. The message is sent.<br>4. The requested information is retrieved on the mobile device.<br>5. A can go back to the public point and proceed to access the service.<br>6. The transaction is closed. |
| Post-Conditions | A receives notification at another selected address or number (later). |
| Variations | ● A calls by audiovisual connection a remote automatic server instead of composing MMS. Cost is increased, test may be performed at remote server. |

| | |
|---|---|
| | ● A may receive instead of a password or key: private information, health test results or an insurance estimation. |
| Asynchronous Actions | A may receive a request for further trials instead of the requested information (authentication gave negative output). |
| Issues | Very sensitive to privacy and then to specific country rules and laws. No direct money risk. Server based. |
| Trust and Threat Issues | ● Data Confidentiality. Confidential information may be transmitted with messages. Data (customer models) are stored on the PS server and this is transmitted with each message to allow authentication of the sender, this data is then deleted locally. This does not reveal useful information that could be used to reverse the authentication algorithm or to interfere with the authentication process. However, special care must taken to ensure that brute force attacks cannot be performed, for instance by limiting the number of times a message from a self-claiming client can be sent in a short period of time.<br>● Data Integrity. Message encryption can provide the necessary level of integrity.<br>● Data Availability. Within the agreed limits of the proposed kind of service, an IP/3G failure for a short period of time (minutes) should not impact the quality of the service. Very urgent communications/alerts should pass through a different service (see Variations, or the first use case above). |
| Requirements | Enrollment control at the bank or hospital (desktop). Test conditions uncontrolled (mobile maybe just avoid very critical environments). Mobile device needs to be enabled to allow composing the necessary message by local test. |

## Who's like you

This use case covers a rather different scenario, when compared to previous ones, as it does not use matching of biometric features for security purposes but for leisure instead. In this sense it is an extremely low risk scenario that can bring a one-time boost in service provider revenue and act as a security service advertisement.

| | |
|---|---|
| UCId | UC005 |
| Use case | Who's like you |
| Description | Users are registered with a provider; they can send an MMS (if possible) or make a multimedia call to upload a set of biometric features. This is used just to find out who's similar to somebody else according to some features calculated and a predefined similarity metric (**not the user model itself**). |
| Actors | - User A (A)<br>- Other User (U) |

| | |
|---|---|
| Assumptions | A is registered with a service provider. A has sent an MMS (if possible) or made an audiovisual call to upload to the server a set of biometric features to be used for the similarity footprint. A is also identified through an ID so that the set of features is uniquely associated with the ID of A.<br>The use exemplifies a case for one other user; it may indeed involve more than one.<br>The service provider has decided a threshold (for instance a score of 80 out of 100) beyond which a notification will be sent to A. |
| Steps | 1. A receives a message on the mobile device containing an ID of matching "bio-friend" U with a score (from 80 to 100).<br>2. A received a message (text) saying that U has left a contact message for him (based on the ID of A he also received in the same way).<br>3. A calls the message box and receives the audiovisual message of U; the mobile device repeats in real-time the test on the received message and the score is displayed.<br>4. A decides to reply to the welcome message and establish a contact with the bio-friend U.<br>5. A drops the audiovisual call. |
| Post-Conditions | None |
| Variations | ● Celebrity matching. In this case the provider may have a contract with celebrity stars or other famous persons offering a service of feature matching with some pre-recorded generic messages. |
| Asynchronous Actions | None |
| Issues | Check if feasible to send biometric-only information via MMS or similar (instead of call).<br>Server based. Nearly no risk involved. |
| Trust and Threat Issues | ● Data Confidentiality. No confidential information should transmitted in this case. The scoring phase is possibly done on avatars and nicknames, not necessarily on real names. Even real contacts at step 4 above may be done with nicknames. Access to real data may be allowed by subscribers under their own responsibility.<br>● Data Integrity. There should be no major issues related to integrity in this kind of service.<br>● Data Availability. There should be no major issues related to availability in this kind of service. |
| Requirements | Enrollment from any devices or Internet databases. Preliminary tests on server. Final test on mobile and/or desktop. |

## 5.2.Summary of Use Cases

The use case scenarios from the previous section are summarized in the table below. In this table

“C” stands for Controlled environment and is typically captured on a Desktop (“D”) using standard or good quality acquisition devices. “U” stands for Uncontrolled environment and can be taken both from a Desktop (PC at home or at work) or from a Mobile (“M”).

| **Use Case** | **Enrollment** | **Authentication** | **Remote Processing** | **Required Security Level** |
|---|---|---|---|---|
| 1 “Bank Order” | C (D) | U (D or M) | Preprocessing on the mobile but authentication on the server | High but can be achieved using an appropriate dialog manager |
| 2 “Secured Chat” | U (D or M) | U (D or M) | All processing embedded on the mobile | Low |
| 3 “Mobile to Mobile” | U (M) | U (D or M) | All processing embedded on the mobile | High but can be achieved using an appropriate dialog manager and reduced, known positive base |
| 4 “Information Retrieval System” | C (D) | U (D or M) | Preprocessing on the mobile but authentication on the server | Medium |
| 5 “Who's like you” | U (M) | U (M) | Preprocessing on the mobile but authentication on the server | Low |

## 5.3.Summary of Trust and Threat Issues

| **Use Case** | **Data Confidentiality** | **Data Integrity** | **Data Availability** |
|---|---|---|---|
| 1 “Bank Order” | Data (customer models) are stored uniquely on the bank server | TLS | Normal telephone call possible |
| 2 “Secured peer-to-peer video chat” | Very low risk that can be eliminated by simple supporting solutions | TLS | Sufficient quality of service can be assured |
| 3 “Mobile to Mobile” | Very low risk that can be eliminated by | TLS if/when necessary. Secured | Sufficient quality of service can be |

| | | | |
|---|---|---|---|
| | simple supporting solutions | data streams are probably not necessary | assured |
| 4 “Information Retrieval System” | Brute force attacks possible; need to block after a few tries | Message encryption | Short periods of unavailability are acceptable. QoS is enough |
| 5 “Who's like you” | Scenario normally based on nicknames and avatars | No major issue | No major issue |

## 5.4.Functional Requirements Emerging from Use Case Specifications

There are several functional requirements that have emerged from the use cases. The functional requirements of most interest for the MOBIO project are those relating to mobile devices. This is because they represent the most challenging cases. A summary of the functional requirements is provided below.

1. The mobile device has to be capable of multimodal calls.
2. For use cases characterized by a high security factor, enrollment can be accepted to be done in a controlled context (controlled environments such as in a bank, hospital or school). When enrollment occurs on a mobile device then the difficulty of the task can be eased by factors like:
   - reduced number of positive customers (for example just the parents of a child)
   - very low security requirements
   - protected environment
3. In most cases test conditions are uncontrolled as they are taking place on a mobile. For high security cases it is acceptable to request that the customer avoid very critical environments (especially in case of money risk or very private informations).
4. The mobile device application should be able to run a simple Dialog Manager; it needs to be enabled to allow composing of the necessary message.
5. The mobile device application must be able to superimpose dialogs and graphic objects on full or partial screen pictures.
6. As a minimum, the remote biometry (see rMoBio above) must be possible on the mobile device and then the device must allow tuning its connectivity settings for a sustained bandwidth in case of communication with the server in the server-based scenarios on a reliable channel (for instance selection among different radio connectivities or joint multiple connections).

# 6.Summary

This documents has provided five use case scenarios. The five use cases were chosen based on a review of consumer needs, market needs and the currently available mobile devices. A review of the currently available mobile biometry has also been conducted which has highlighted the need for unintrusive mobile biometric technology.

From the use case study it is concluded that data collection for the enrollment should be done from both a mobile and desktop (or laptop). Also, the data that is collected for testing should be obtained only from the mobile as this corresponds to the more general and more challenging use cases.

The device overview combined with project requirements has highlighted several possible devices. Unfortunately, two of the best mobile devices have to be discarded, the iPhone and the Meizu M8. The iPhone cannot be considered as it does not have any frontal camera. The Meizu M8 also has no frontal camera and it is not currently available, it is also questionable in terms of reliability. The N96 also had to be discarded as it is not yet available and operates a more complicated OS, the Symbian OS, which has more demanding development requirements. This still leaves several available mobile devices.

It is foreseen that initial development will occur using the HTC S730 or a similar device. This device is considered to be the most likely option as development work will be much quicker on this device; it's important to note that this device also meets all the necessary requirement. The quicker development time is due to the fact that it uses the Windows Mobile OS and also that EyePMedia has experience with previous versions of the HTC devices.

# 7.Acknowledgments

The author would like to thank Sebastien Marcel and Christopher McCool (IDIAP), Jean-Francois Bonastre (UAPV), Honza Cernocky and Pavel Matejka (BUT) for their contributions and review.