*Journal of Multimedia Information System: ISSN 2383-7632(Online)*
*VOL. 1, NO. 1, September 2014, pp. 23-43*

# Security Model for Pervasive Multimedia Environment

Benchaà Djellali[1,2], Pascal Lorenz[1,*] , Kheira Belarbi[2], Abdallah Chouarfia[2]

## Abstract

With the rapidity of the development on electronic technology, various mobile devices are produced to make human life more convenient. The user is always in constant search of middle with ease of deployment. Therefore, the development of infrastructure and application with ubiquitous nature gets a growing keen interest. Recently, the number of pervasive network services is expanding into ubiquitous computing environment. To get desired services, user presents personal details about ¬his identity, location and private information. The information transmitted and the services provided in pervasive computing environments (PCEs) are exposed to eavesdropping and various attacks. Therefore, the need to protect this environment from illegal accesses has become extremely urgent. In this paper, we propose an anonymous authentication and access control scheme to secure the interaction between mobile users and services in PCEs. The proposed scheme integrates a biometric authentication in PKI model. The proposed authentication aims to secure access remote in PCE for guaranteeing reliability and availability. Our authentication concept can offer pervasive network service users convenience and security.

**Key Words**: Security, PCEs, PKI model, Information transmitted.

## I. INTRODUCTION

The lower cost of components and their miniaturization make possible a world in which the electronic is likely to be incorporated into any object. Technically, the addition of a chip in an object doesn't represent any particular difficulty and economically, add a chip and an embedded small program in an object is not a commercially prohibitive cost. In term of use, the additional service rendered is simple, easily discernible by the user and is quite justified. Thus, instant communication implementation to our service of panels indicators, screens or communication devices as soon as we step across the threshold of a home, a hotel bedroom , a warehouse or a public space is the essence of ambient intelligence [1, 2] and pervasive networks [3].

The ubiquitous network [4, 5] is the support of transparent collaboration between equipment which constitute it collectively and permanent cooperation of the network of personal objects of every individual who crosses its threshold. The ubiquitous network is a network of continuity which must, as the origin of its name indicates, be present everywhere, all the time and this without breaking. Nevertheless, in an environment where by default each object will be connected and accessible, arise necessarily issues of confidentiality, privacy and non-intrusion [3].

A pervasive network includes a variety of network protocols and is expected to support many service models such as a client-server model, a peer-to-peer communication model, and hybrid model. For that, it is difficult to definitely decide which mechanism is suitable for pervasive network. Despite all this, many types of authentication methods such as ID-password-based authentication method, certificate-based authentication method, and biometric information-based authentication method are used to secure the interaction between mobile users and services and allow only legitimate users in PCEs.

Therefore, biometric information-based authentication method is revealed very promising since proposed biometric keys are based on physiological and behavioral characteristics of persons such as fingerprints, faces, irises, hand geometry, and palm prints [6, 7, 8]. Furthermore, biometrics-based authentication is inherently more reliable than traditional password-based authentication.

Manuscript Received August 12, 2014; Revised September 05, 2014; Accepted September 26, 2014. (ID No. JMIS-2014-0004)
Corresponding Author (*): Pascal Lorenz, University of Haute-Alsace, lorenz@ieee.org.
[1]University of Haute-Alsace, Colmar, France. E-mail: benchaa.djellali@uha.fr, lorenz@ieee.org.
[2]University of Sciences and Technology of Oran (USTO-MB), Algeria. E-mail: belarbi_khe@yahoo.fr, chouarfia@mail.com.

The advantages of biometric keys can be resumed by the following properties:

- Cannot be lost or forgotten.
- Very difficult to copy or share.
- Extremely hard to forge or distribute.
- Cannot be guessed easily.
- Not easy to break.

In this context, Lee et al. [9] proposed a fingerprint-based remote user authentication scheme using smart cards, but this scheme could not withstand impersonation attack [10, 8]. Lin and Lai [8] further proposed a flexible biometrics remote user authentication scheme. However, this scheme is susceptible to the server spoofing attack [6]. Li and Hwang [11] presented a biometric-based remote authentication scheme. The proposed scheme can be suitable for various authentication cryptosystems in distributed computing environment.

In this paper, we propose a security framework for pervasive network in order to safeguard against wide range of threats. The proposed model basically involves a user authentication and an authorization mechanism for controlling access.

The user authentication mechanism is based on biometric-based authentication [11]. We adapt this scheme to pervasive computing environment by integrating it into an infrastructure composed of authentication and authorization authorities to allow access to the different services offered in a pervasive network.

The remainder of this paper is organized as follows: In section 2, we present the pervasive computing environment: We discuss the characteristics and the security challenges. In section 3, we speak about trust models, user's privacy preservation and digital and biometric identification. In section 4, we return to biometrics and its technology in front of traditional authentications methods. In Section 5, we propose a security infrastructure model for pervasive computing environment and a security protocol based on biometric authentication and authorization. The security and the efficiency of our scheme will be analyzed in Section 6. Finally, we conclude with further research guidelines.

## II. PERVASIVE COMPUTING ENVIRONMENT

Microprocessors are embedded in the everyday object we use but we are largely unaware of it. Marc Weiser [12] put forward the view that ubiquity will have been achieved only when computing has become invisible and there is intelligent communication between the objects that anticipate our next move. After that, technology has advanced along many dimensions, especially in hardware progress and wireless communication technologies. A number of leading technological organizations are exploring Pervasive Computing Environment. But it is far from Weiser's vision become reality. Pervasive Computing will be the future. Pervasive computing will be a fertile source of challenging research problems in computer systems for many years to come [13].

### 1. Characteristics of Ubiquitous Networks

#### 1.1 Heterogeneous Characteristics

The ubiquitous network is a combination of technologies and services offered by the cable, wired and mobile telephony, wireless and satellite which could quickly lead to reliable and complete network coverage. The tools deployed indoor the pervasive network vary between the smallest device with reduced autonomy and capacity of processing and storage, and the sophisticated, powerful and very fast computer. The ubiquitous network infrastructure is conceived to offer ideal conditions of interconnection of variety of heterogeneous components, so that services and applications are accessible at anytime, anywhere and in any condition of the network environment [14].

#### 1.2 Dynamic and Self-Organizing Characteristics

A pervasive network is characterized by a self-organization and dynamism of offer and demand: From a wide choice of suppliers, it offers a wide variety of services. These services could be utilized by a variety of different ubiquitous network users' devices. Ubiquitous network users move easily in the network and enjoy a dynamism which enables them to join or leave instantaneously the network. They can travel from one network to another without obstacle. But, each network has its management peculiarity and its security policy. For that, the passage from one network to another triggers automatically a dynamic reconfiguration in order to make it possible to transiting users to take advantage of the offerings of the networks of which they cross [14]. A service provider may at any time become a user of other services and vis-versa a service consumer can become in turn a service provider. To note that certain services provided by the ubiquitous network as TV, multimedia and video on demand, require a quality of service which should be supplied by the ubiquitous network or the network on which is built the ubiquitous network.

#### 1.3 Invisibility and Smartness Characteristics

A system that requires minimal human intervention offers a reasonable approximation of invisibility. Humans can intervene to tune smart environments when they fail to

meet user expectations automatically. Such intervention might also be part of a continuous learning cycle for the environment and the environment and the objects in it must be able to tune themselves to meet user expectations continuously. The ubiquity will have been achieved only when computing has become invisible and there is intelligent communication between the objects that anticipate user moves and expectations. Smartness involves accurate sensing followed by intelligent control or action between system entities.

**2. Security in Ubiquitous Networks**

The security of pervasive computing environment refers to establish mutual trust between infrastructure and device in a manner that is minimally intrusive. In such environment, a close relationship binds any smart device to its owner who by a universal remote control that kept secured, is recognized by the smart device. When user deploys device, secure transient association is used and imprinting can be used to establish shared secret. However, control gain of users' devices by a hacker, eavesdropping of communication channels, modification of sensitive commerce transactions, DoS, transaction of services or goods in other identities, are among numerous threats that are difficult to track and secure in ubiquitous networks.

Thus, ubiquitous network infrastructure will require the provision of certain degree of security between participating user devices. And therefore, there are interesting and challenging problems in providing consistency in the management of security and in specifying authorization policies for pervasive computing environments.

Security can be implemented in heterogeneous components such as firewalls, different computer operating systems and multiple databases. The pervasive computing system should support secure sensitive or high-value transactions and verifies that messages were not modified while in transit from queue to queue.

Authentication is one of the most important characteristics of ubiquitous computing security. Authentication provides confirmation of user access rights and privileges to the information to be retrieved. During the authentication process, a user is identified and then verified not to be an imposer. The authentication process is the assurance process that a party to some computerized transaction is not an impostor [13].

**3. Security Challenges in Ubiquitous Networks**

The ubiquitous network is nowadays almost at hand. The combination of technologies and services offered by the cable, wired and mobile telephony, wireless and satellite could quickly lead to reliable and complete network coverage. For that fact, hopes on pervasive computing environments do not cease to increase. Nevertheless, challenges remain very important and the challenge string touches all stages of service life cycle. Traditional security requirements include authentication, authorization and confidentiality. The security must be defined in terms of services themselves, the way they are dynamically added and removed, the way they are discovered and delivered, and their availability. In the other side, a service consumer expects from the system its peculiarity protection and a maximum of available service with a free access. Between service and consumption, the problem is likely to be complex and interest conflicts may be generated.

**Confidentiality:** Interactions between user and service should have guarantees of confidentiality and integrity whenever these protections are necessary. Ubiquitous network management information needs to be protected in storage and during transmission. Such protection is usually realized through password or cryptographic technique. The challenge to come to deploy indeed large-scale the ubiquitous services is how to get adequate provisions for handling user's confidentiality. The preservation of user's confidentiality is a much more difficult task in an environment that is at the stage of discovery and at structuring research of its security. The proposed infrastructure and the techniques developed currently for pervasive networks are promising.

**Authentication:** In a pervasive network, authentication is the most important security service. It allows an entity to verify the identity of another entity. Direct or indirect mutual authentication between user and service provider should be established in advance. This authentication spreads a relationship of trust. Subsequently, a user questions only real authenticated service and a service provider responds to only authenticated user.

**Authorization:** Services providers' trough ubiquitous devices are beforehand authorized to supply services and users will obtain by the suite the access rights to these peripherals.

**No repudiation:** the present mechanism in ubiquitous environment has to prevent an entity from denying the previous commitments or the expected actions from him.

**Privacy and anonymity:** In an environment with an important concentration of devices, the users should rightly be concerned with their privacy. A pervasive environment must preserve user's privacy. The real identity of a user will have to never be revealed in communication exchange between user and server expected if it is voluntary revealed by the user. In

pervasive computing environment, the quests for authentication, access control and users privacy protection often enter in conflict in many aspects and make the problem more complex. A service to provide in PCE depends generally on the user identity contour and the pre-established trust relationship to realize user authentication and proceed to access control. On the other hand, user does not want to be followed by the service everywhere he is and all what he does. The compromise between the two thus raises a big challenge to the security designers of pervasive network.

**Availability:** The elements belonging to a pervasive network enjoy a dynamism which enables them to join or leave instantaneously the network. This dynamic change will not have to penalize the ubiquitous network management functions. To note an instantaneous exit of an entity which ensures an authentication task will have a negative effect on the behavior of the pervasive network and its security. The pervasive network has to insure that network resources or services are available and protected against attacks. Because of the difference in security policy sometimes imposed by neighboring networks and for reason of compliance, a dynamic reconfiguration of users joining or leaving a network is triggered automatically. And due to the dynamism, ubiquitous network users' devices will requires simple and fast authentication computations, as they join, leave and join the ubiquitous network [14].

**Interoperability:** A pervasive network is generally composed of heterogeneous components and particularly of elements belonging to domains equipped with local security. For that, the security for ubiquitous network architecture needs to be compatible with existing local security solutions.

**Attack Unobtrusive Withstand:** With the variety of heterogeneous component composing the ubiquitous network, attack by malicious nodes in any point of network can easily happen. The challenge is to prevent attacks by incorporating appropriate security protocols and managing credentials in a manner that end-to-end security is achieved from the user's perspective, as unobtrusively as possible.

## III. PRIVACY AND TRUST MODELS

### 1. Characteristics of Ubiquitous Networks

Different degrees of trust may be required for different users and their devices to access services in ubiquitous networks. These will be reflected in the ubiquitous network record and resources to determine whether the users and their devices are authorized to access. Applications implemented must be trusted to operate correctly and have full privileges to access the network and devices' resources. Trust models that are based on real world and social properties to identify trustworthy entities and develop capability to reason about trust [15] are required in ubiquitous networks. Thus, security architecture for ubiquitous network environment should be designed to allow safe execution of trusted applications in a real world and social scenario. In addition to trusted environment, a robust reputation system [16] is required for misbehavior detection for ubiquitous network environment [14].

### 2. Privacy

Protecting the privacy of users is of central importance. But, how is privacy maintained when location and activity are tracked and perhaps predicted or sensed by the environment? In a ubiquitous computing environment, sensors are actively collecting user data, much of which can be very sensitive and valuable.

Personal data have become particularly vulnerable to the development of new technologies. In this context, many regulations attempt to ensure the security of information systems and the protection of user's privacy. However, the standard protections ensuring the security of information systems are inadequate; we must also develop requirements for privacy in order to protect personal information.

At present, three privacy principles have been developed:

- Data sensitivity principle: The processed personal data are considered to be sensitive and require a decentralized structure for their storage.
- Data sovereignty principle: The personal data belong to an individual and require a control and an authorization on their uses and their purposes.
- Data minimization principle: The personal data disclosure should be limited to adequate, relevant and not excessive data. It includes anonymity and untraceability.

The requirements for privacy respect are numerous in an information system. Four constraints have been described in the functional requirements of the common criteria [17]: anonymity, pseudonymity, untraceability and non-observability. More precisely, the anonymity ensures that a user can access a resource without disclosing his identity, while pseudonymity requires that the person be responsible for this use. The non-associability concept guarantees that personal data are protected against an aggregation procedure. This concept is related to anonymity. Indeed, the data association can optionally allow recovering the identity of an individual. Moreover, it must add to this principle, the possibility for an attacker to retrieve a data outside the system. The untraceability is therefore not an elementary principle because distributed

Data across different organizations can be correlated.

**3. Traditional authentication and PCE:**

Most traditional authentication methods cannot be applied as it is in ubiquitous computing environment. The reasons of why traditional authentication methods do not fit are that these methods cannot scale well with hundreds or thousands of embedded devices that placed in highly distributed environment such as ubiquitous computing environment. They are not convenient for users walking around within ubiquitous computing environment. Furthermore traditional authentication method that focus on identity authentication, possibly will fail to work in ubiquitous computing environment, since it conflicts with privacy protection which is one of the most important user's concerns in ubiquitous computing environment. Authentication in pervasive computing environment requires different methods to cope with its different requirements, context and applications. Also authentication requirements are highly varied for different applications [18, 19, and 20].

**4. Authentication devices for UCE:**

The authentication devices can be used integrated or alone in PCE. Between the authentication devices the most convenient and the most suitable for the PCE, we can identify [18]:

• Active Badges: In some Pervasive Computing Environment, each person has an active badge that can transmit the information of identity.

• Smart Jewelry: People can ware Jewelry at all times, so it is harder to be stolen and does not necessitate a user to carry other gear. For that reasons, programmed jewelry can offer a convenient authentication method. The iButton is an example; it is a 16mm computer chip in a stainless steel case. Also, it allows up-to-date information to move with user or object. The steel button is strong enough to resist insensitive outdoor environments.

• Smart Watches: A wristwatch is another wearable device that is worn by people almost all the day. A “smart” watch can be considered as an interactive wearable device, it provides a higher degree of security in authentication. In contrast to the previous wearable devices, smart watches store more information, have more processing power, have display features and make possible for user to interact with the device. Smart watch considered as secure authentication device because of these features make.

• PDAs: Larger PDAs are also used for authentication purposes as well as the wearable gadgets. The PDAs devices provide more feature i.e. more storage capacity and more processing power. Even as PDAs can be stolen or lost more easily than wearable devices like gadgets, they can be utilized to provide better authentication according to their processing, storage and interactive displays.

• Passwords: The traditional authentication method uses username and password pairs can be usable as a supplementary authentication method that can leverage other authentication methods.

• Biometrics: Biometrics could be used as an efficient mean of authentication. The users will be authenticated based on their distinctive physical characteristics, in order that users are identified according to “what they are.” This may include retina, fingerprints, and face or voice recognition.

**5. Authentication models**

Basing upon the basic foundations of the access control and the preservation of privacy, we can group the authentication models in term of security properties in:

**5.1. Model built over Kerberos**

The proposed general security framework is built over Kerberos and establishes new enhancements that let it to blend nicely into pervasive computing environments, and identify general security requirements. The focus is on designing specific infrastructure for security to protect user context privacy from the service providers. A MIST infrastructure is used and provides anonymity for user through an overlay network also it keeps all information of all the users using what they call “Lighthouse” [18, 20].

In this model, designers make the Active Space able to detect the presence of users and objects actively. These features are necessary to make spaces active and to enable context-based applications. The used method allows users to be authenticated to the surrounding environment and simultaneously preserves their privacy. The Mist communication infrastructure is established in the pervasive computing environments to preserve location privacy, while allowing users and objects to be authenticated at the same time [18]. Using Mist Infrastructure, confidentiality is achieved. It also provides integrity protection for the communications between the mobile user and the service [21].

• Mist: consists of a hierarchy of Mist Routers that structure an overlay network. This network allows private communicate for users. The Mist Routers route packets using a hop-by-hop, handle-based routing protocol with limited encryption using public key cryptography, as a consequence, the communication become untraceable by eavesdroppers.

• Authentication Protocol: authentication protocol in

this model extends Kerberos authentication protocol to support user devices and make use of the location privacy that provided by Mist. In each Active Space, they assume the existence of “Space Authentication Portals” (SAPs), which are special types of Portals that could be located at the Active Space entrance, or other suitable places. The SAP will feature a set of wired and wireless base stations and device readers that allow users to be authenticated with the Active Space using any authentication devices they are wearing or carrying.

In this model, all users have active badges. The badge programmed to store unique ID number, for user identification, and store ID for user's Lighthouse identification. Then user comes close to one of the available SAPs for authentication. Some of the authentication devices possibly will require the intervention of user, e.g. insert the iButton into the corresponding designated receptor. Then the communication is done through Mist communication, so the lighthouse communicates with the Security Server. Note that SAP does not have sufficient information for user's authentication. Upon authentication success, the AS, like Kerberos protocol, produces a ticket granting ticket (TGT) for that user. The TGT is issued for a user is encrypted and stored in the users Lighthouse. The AS remembers the user's previous authentication methods and then calculates the net confidence of all authentication methods of the user being there to issue new TGT with the new value. After that, the user can access the service, but the service needs to check the user first by contacting with the user's Lighthouse. Using the TGT that are stored in the Lighthouse of user, the Lighthouse will communicate with the TGS and request for tickets to access the requested service. These tickets are encrypted and do not contain any indications to the real identity or name of the user; they incorporate a pseudonym. Also, they contain the net confidence level and the security privileges of the user, so the service can make access control decision whether to authorize that user or not. When the user exit from the room the badge reader at the exits can discover that and automatically it will log off the user and destroy the stored tickets in his Lighthouse [18, 20].

### 5.2. Model based on hash chain and blind signature

This model proposes a scheme to secure the interactions between services and mobile users in pervasive computing environment. The scheme integrates two fundamental cryptographic primitives: the hash chain and the blind signature into authentication protocol. These techniques can be described as follows:

• Blind Signature: The blind signature is one of the digital signature variations where the message content disguised from the signer. It can be implemented based on some well-known digital signature schemes. A user first use a random “blinding function” f, to “blinds” the message before sign it from third party. So the signer will sign the message without having any idea about its content, and then send it back to user. The user unblinds the message and obtains the signature on the original message. Blind signature used for non-linkability property, and this property is helpful when anonymity is required [19].

• Hash Chain: also called one-way hash function is one of the powerful cryptographic tools. It takes a message of any size as input and outputs a fixed size hash. A chain of hash outputs can be obtained by applying repeatedly on an initial message. And the outputs of hash can be used in the reverse order of generation for authentication purpose. [19]

Sample system architecture of a pervasive computing environment, generally, consists of three types of entities: the Mobile users, the Services and the Back-end authentication servers, besides, the underlying wireless and wired communication infrastructures. While the wireless network access is a service by itself. Protecting the user privacy includes protection from the outsiders and from the network service providers. The proposed access control in this model is designed to secure the interactions among these three types of entities [19, 20].

Table 1 resumes in term of security properties the comparison between the Kerberos based model and the hash chain and blind signature based model.

Table 1. Models security features comparison

| Security Property | *Kerberos-Based Model* | *Hash-chain-and-blind-signature-Based Model* |
|---|---|---|
| Mutual Authentication | No | Yes |
| Concrete Protocol | No | Yes |
| User Context Privacy | Yes | Yes |
| Differentiated Service Access Control | Yes | Yes |
| Integrity | Yes | Yes |
| Confidentiality | Yes | Yes |
| Provable Security | Yes | Yes |

## 6. Digital Identity

An identity is represented by a sufficient number of attributes to identify an individual in a given population with known general characteristics. The management of identities consists of "systems and processes that manage and control those who access resources and what each user is entitled to do with these resources, this in accordance with the Organization's policies" [22]. The person related to this digital identity is responsible of his acts. Identity theft is therefore a significant threat for users [23].

Effective solutions for controlling access to data in such technology-rich environments remain to be a challenge for some time to come.

**7. Biometric Identity**

In constant evolving in digital world, secure and privacy preserving management of our digital identities, is of paramount importance to citizens, industries, social groups and Governments. Numerous applications are emerging related to physical access control (buildings, restricted areas ...), logical access points (bank accounts, tax payments ...) or identity documents (passport, national identity card...). In order to achieve more secure systems, biometric technologies are employed in an increasing manner in order to verify the identity of a user by performing an authentication or to find out his identity by identification tasks. The major reason for this widespread use of biometrics is that this technology provides the strongest proof of the physical presence of a person.

However, with more and more applications using biometrics, new privacy and security risks arise. And questions like “What can I do if my biometric data has been stolen or misused?” require urgent attention not only to reassure users with regards to privacy intrusion but also to prevent misuse and improve accuracy. Standard biometric templates are permanently associated with an individual; they are increasingly used in that they can be compromised. Since they cannot be replaced, they are also inherently non revocable. This makes classical biometric systems inappropriate for privacy and security critical applications. Therefore, these major issues of biometric systems that guarantee the rules of privacy protection should be solved urgently.

Recently, different architectures have been proposed by academics and industries [24] in order to guarantee some security issues such as the storage of applications and data in a secure way in different devices such as mobile phones or smart cards. This trusted architecture is the ideal support for storing biometric templates for security reasons and also because this can be done in a post-personalization way. Over the last decade, a new innovative multidisciplinary research field has emerged, that combines biometrics and cryptography, and that has the capability to guarantee biometric data privacy in an algorithmic way. The resulting innovative hybrid systems have the following important properties: they confer to biometric characteristics the needed capabilities of revocability, privacy, and diversity, and provide cryptographic systems with a strong link to the user through biometrics [25].

# IV. BIOMETRICS AND AUTHENTICATION

**1. Biometrics Presentation**

**1.1 Biometric Characteristics**

The biometric characteristics by which it is possible to verify the identity of an individual are known as biometric modalities. Figure 1 shows an example of some biometric modalities. The variety of biometric modalities available is based on the analysis of individual-related data and is generally classified in three broad categories: biological, behavioral and morphological biometrics characteristics.
Biological biometrics is based on the analysis of biological data relating to the individual such as DNA, saliva, cardiac signals [26], Electroencephalogram signals [27], etc.

- Behavioral biometrics is based on analysis of behaviors of an individual such as voice, keystroke dynamics [28], way of walking, etc.
- Morphological biometrics is based on specific physical traits that, for all persons, are unique and permanent such as fingerprint, face, iris, hand veins [29], etc.

Practically, any morphological or behavioral characteristic can be regarded as a biometric characteristic, insofar as it satisfies the following properties [30]:

- Universality: all persons to be identified must possess;
- Uniqueness: the information must be as dissimilar as possible among different persons;
- Permanence: the information collected must be present during the lifetime of an individual;
- Collect-Ability: the information must be collectable and measurable in order to be used for comparisons;
- Acceptability: the system must respect certain criteria (ease of acquisition, quickness, etc.) to be used

The biometric characteristics do not possess all these properties, or possess them, but at different degrees. Table 2 compares the main biometric modalities according to universality, uniqueness, permanence, collect-ability, acceptability and performance properties [31]. No feature is therefore ideal and that they can be more or less adapted to specific applications. For example, the DNA-based analysis is one of the most effective techniques to verify an individual's identity or identify him. Nevertheless, it cannot be used for the control of logical or physical access for reasons of calculation time, but also, because nobody would be willing to give a little blood to do the verification. The modality choice is thus carried out

according to a compromise between the presence or absence of some of these properties according to the needs of each application. The biometric modality choice may also depend on the local culture of the users. In Asia, the methods requiring physical contact such as fingerprints are rejected for reasons of hygiene while non-contact methods are more widespread and accepted.


Fig. 1. Biometric modalities

### 1.2 Biometric Templates

A biometric template is the set of data used to represent a user. The acquired biometric characteristics are not recorded and used such they are. A processing phase is performed to reduce raw biometric data and produce thereby a biometric template. Figure 2 illustrates some examples of biometric templates. For storing templates, there are four main locations which are an USB key, a centralized basis, an individual work machine and a biometric sensor. Each of these locations has advantages and weaknesses in terms of processing time, confidentiality and privacy respect. In France, the use of the centralized basis is prohibited by the National Commission of data processing and freedoms (CNIL) for a large number of individuals.

The scope of biometrics is very extensive. Indeed, all fields that require check or determine the identity of persons are concerned. Thus include biometrics applications to manage access to physical resources (such as access to secure sites) and logical (such as e-commerce). Biometrics interests also several countries (Europe, United States, etc...) to produce more secure identity documents, such as the national identity card or biometric passport. It should be noted that in France and in Algeria, the biometric passport is now deployed. It incorporates a RFID chip that contains at least two biometric information: a fingerprint and a digitized facial image. Finally, biometrics has not only safe oriented applications, but also applications that facilitate the daily lives of users. Thus, biometrics is used in some airports to avoid to regular customers wasting time during boarding. Performed according to the International Biometric Group statistics [32], Figure 3 shows the market shares of the main biometric methods in 2009. Fingerprints are the most used, followed by facial recognition. These two modalities represent three quarters of the biometrics market.

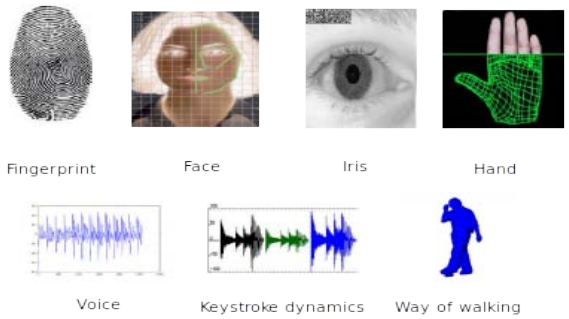


Fig. 2. Biometric templates

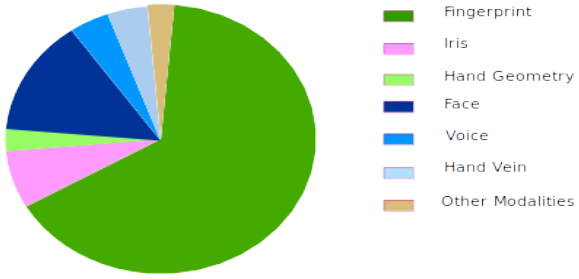


Fig. 3. Market shares of the main biometric methods.

### 1.3 Biometrics and Traditional Authentication Methods

Biometrics has an important advantage over traditional methods in the sense where it avoids the use of a large number of complex passwords, badges, etc. Table 3 presents a parallel between biometrics and the traditional authentication methods. This table shows that biometric systems facilitate the authentication process and resist to the various existing attacks on secret based systems or on possession based systems. However, these systems may present disadvantages regarding the privacy respect and the information biometric uncertainty. A comparison of these techniques is detailed by O'Gorman [33].

## 2. Biometric Technology

### 2.1 Enrolment, verification, and identification

Biometric systems operate in three modes:

**a) Enrolment**

Table 2. Biometric modalities comparison [31]

| Information | Universality | Uniqueness | Permanence | Collect-ability | Acceptability | Performance |
|---|---|---|---|---|---|---|
| ADN | Yes | Yes | Yes | Weak | Weak | ***** |
| Blood | Yes | No | Yes | Weak | No | * |
| Approach | Yes | No | Weak | Yes | Yes | *** |
| keystroke dynamics | Yes | Yes | Weak | Yes | Yes | **** |
| Voice | Yes | Yes | Weak | Yes | Yes | **** |
| Iris | Yes | Yes | Yes | Yes | Weak | ***** |
| Retina | Yes | Yes | Yes | Yes | Weak | ***** |
| Face | Yes | No | Weak | Yes | Yes | **** |
| Hand geometry | Yes | No | Yes | Yes | Yes | **** |
| Ear | Yes | Yes | Yes | Yes | Yes | ***** |
| Fingerprint | Yes | Yes | Yes | Yes | Average | **** |

Enrolment is the first phase of any biometric system. This is the stage during which a user is registered in the system for the first time. It is common to verification and identification. During enrolment, the biometric characteristic is measured using a biometric sensor to extract a numeric representation. This representation is then reduced, by using a well-defined algorithm of extraction, to reduce the quantity of data to store to facilitate so the verification and the identification. Depending on the application and the desired level of security, the biometric model chosen, is stored either in a central database, or on a personal element appropriate to each person;

**b) Verification**

The identity verification consists in controlling if the individual using the system is indeed the person that he claims to be. The system compares the biometric information acquired with the corresponding biometric template stored in the database, we speak about test 1. In this case, the system returns only a binary decision (Yes or No) that can be weighted. The verification process can be formalized as follows:

Let CU be the vector defining the biometric characteristics of the user U extracted by the system, and MU be its biometric template stored in the database. The system returns a Boolean value further to the calculation of the function f defined by:

$$f(C_U, M_U) = \begin{cases} 1 & \text{if } S(C_U, M_U) \geq \tau \\ 0 & \text{else} \end{cases}$$

where S is the function of similarity defining the correspondence between both biometric vectors and $\tau$ the threshold of decision from which both vectors as considered as identical.

**c) Identification**

In identification mode, the biometric system determines the identity of an unknown individual from a database of identities, we speak about test 1. In this case, the system can attribute to the unknown individual the identity corresponding to the nearest profile found in the base (or a list of similar profiles) or reject the individual. The Identification process can be formalized as follows:

Let CU be the input vector defining the biometric characteristics extracted by the system for a user U who presents himself. The identification means to determine the identity of $I_t$, $t \in \{0, 1, \bullet\bullet\bullet, N\}$ where $I_1, \bullet\bullet\bullet, I_N$ are the identities of the users previously enrolled in the system and

$I_0$ indicates the unknown identity. The identification function f can be defined by:

$$f(C_U) = \begin{cases} I_k \text{ if } \max_{1\leq k\leq N} S(C_U, M_k) \geq \tau \\ I_0 \text{ else} \end{cases}$$

where $M_k$ is the biometric template corresponding to the identity $I_k$, S the similarity function and $\tau$ the threshold of decision.

Table 3. Biometric authentication and password/key comparison.

| Biometric Authentication | Password/Key Authentication |
|---|---|
| - based on biological, behavioral and morphological measurements<br>- ease to use ( no secret to remember)<br>- individual authentication<br>- information in permanent and close relationship with the user<br>- use a probabilistic comparison<br>- Biometric information can be modified or faded by the time: uncertainty<br>- privacy respect problem<br>- Difficult to revoke information | - Based on that we know or have<br>- Can be more complicated (complex passwords)<br>- Authenticate the key<br>- Can be lost, stolen or forgotten<br>- Use an exact comparison<br>- Information Does not vary: Surety<br>- Less impact on privacy<br>- Easy change |

### 2.2 Architecture of Biometric System

Biometric system architecture contains five modules:

- Capture module: It is a biometric sensor with or without contact which acquires biometric data in order to extract a digital representation. This representation is then used for enrolment, verification or identification.
- Signal processing module: It allows reducing the digital representation extracted to optimize the quantity of data to be stored during the enrolment phase or to facilitate the processing time during the verification and identification phases. It can have a quality test to control the acquired biometric data.
- Storage module: It contains the biometric templates of the users enrolled in the system.
- Similarity module: It compares the biometric data extracted by the capture module to one or more templates previously stored. It determines the similarity or divergence degree between two biometric vectors
- Decision module: It determines whether the similarity index returned is sufficient to determine the identity of the individual [34].

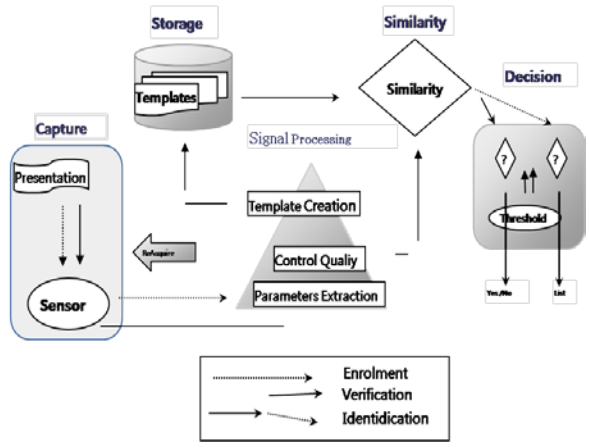


Fig. 4. Genetic architecture of biometric system.

## V. SECURITY INFRASTRUCTURE MODEL FOR UBIQUITOUS NETWORKS

### 1. Security System Models

The pervasive network is comprised of pervasive network users, smart devices, smart network services, and smart gateway which is supposed to be responsible for the security of every pervasive and do therefore a central role in the pervasive network.

The security infrastructure of a pervasive network essentially boils in smart gateway. Every smart gateway consists mainly of an authentication entity, an authorization entity and a security policy. Through their close cooperation, these entities secure access to pervasive network components. Such infrastructure is installed in each domain of the ubiquitous network and all pervasive network packets must pass through it. Whenever a new pervasive network access is detected, it should be able to authenticate, authorize and enforce security policy [36, 37].

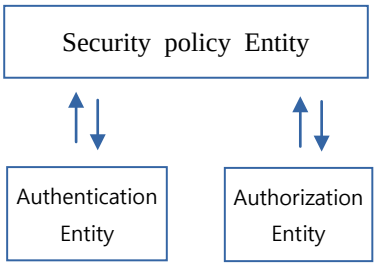


Fig. 5. Security infrastructure for pervasive network.

In order to strengthen the authentication and authorization mechanisms, security policy rules are managed by the security policy entity. The administration of this entity can vary between an intelligent and automatic generation of rules depending on the needs and the behavior authentication and authorization entities, and

the intervention of authorized agent. These rules strengthen particularly the decision-making of the security entities and generally the pervasive network security.

Based on these rules, the authentication and authorization entities authenticate and authorize users or devices accessing the pervasive network [37, 38, 39]. Figure 5 shows the security entities of a smart gateway.

In order to provide service to only legitimate members and make each user of the pervasive network reliable and able to use safely the pervasive network services, the pervasive network needs to authenticate entities that are accessing pervasive network. Initially, the authentication and authorization entities share a common secret. Any ubiquitous registers its service with the authorization authority. This latter transmits a secret service.

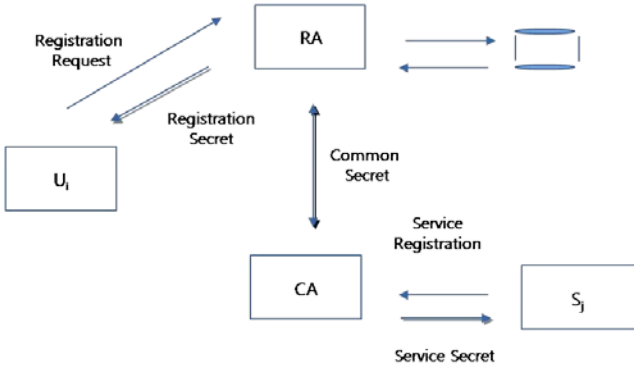


Fig. 6. Process of entities collaboration

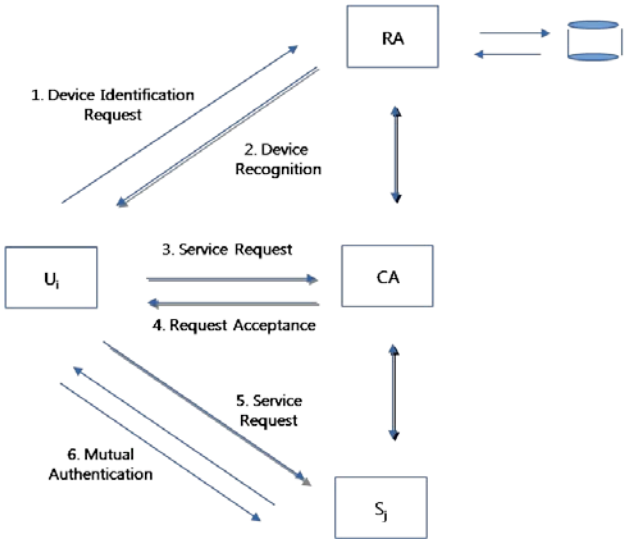


Fig. 7. Process of device authentication and authorization.

A user accessing the pervasive network registers with the authentication authority. It generally transmits to this effect its identity, password, or biometric information. The authentication entity transmits a hidden secret that will serve later for authentication. Figure 6 represents the main stakeholders in a pervasive network and initialization and registration interaction.

The authentication and authorization process is initiated by an authentication request from an entity which may be a pervasive network user or a smart device. Based on registration information, the authentication entity responds by device recognition or a reject. The response contains a hidden and shared secret between the authentication and authorization entities. As result, user queries the authorization entity a service among the services offered by the pervasive network. This query contains the hidden and shared secret between the authentication and authorization entities. In turn, the authorization entity answers by a request acceptance that contains the hidden service secret. Upon response reception, the user smart device sends a service request that contains the hidden service secret to the smart network service. A mutual authentication is launched between smart network service and smart device or user.

The authentication and authorization process is initiated by an authentication request from an entity which may be a pervasive network user or a smart device. Based on registration information, the authentication entity responds by device recognition or a reject. The response contains a hidden and shared secret between the authentication and authorization entities. As result, user queries the authorization entity a service among the services offered by the pervasive network. This query contains the hidden and shared secret between the authentication and authorization entities. In turn, the authorization entity answers by a request acceptance that contains the hidden service secret. Upon response reception, the user smart device sends a service request that contains the hidden service secret to the smart network service. A mutual authentication is launched between smart network service and smart device or user

The authentication and authorization process is initiated by an authentication request from an entity which may be a pervasive network user or a smart device. Based on registration information, the authentication entity responds by device recognition or a reject. The response contains a hidden and shared secret between the authentication and authorization entities. As result, user queries the authorization entity a service among the services offered by the pervasive network. This query contains the hidden and shared secret between the authentication and authorization entities. In turn, the authorization entity answers by a request acceptance that contains the hidden service secret. Upon response reception, the user smart device sends a service request

that contains the hidden service secret to the smart network service. A mutual authentication is launched between smart network service and smart device or user.

Figure 7 plots the authentication and authorization dialogue between pervasive network components namely user smart device, smart network service, and authentication and authorization authorities.

The indoor pervasive network user controls smart devices and access smart services via smart gateway. A mobile user is connected to the smart gateway of the domain which it depends. Thus, the Users of the pervasive network will safely use the services of the pervasive network and the pervasive network services are issued to only legitimate users.

In order to allow continuity of service for roaming user, secure communications are made between smart gateways of the surrounding areas. Remote access of an external user to the pervasive network is another possible option. It consists in connecting that user to a smart portal server. The latter is connected to the smart gateway of the pervasive network of the desired service.

The smart gateway of the pervasive network functions as a gateway between the closed pervasive network and the outside world either by communicating with different smart gateway neighboring either by communicating with a smart Portal Server.

Gateways of different domains of pervasive networks share mutually secrets that enable them to Exchange safety information of users transiting from one domain to another and requesting service. This secure exchange will allow an identified user in one domain to be authorized to receive service in another domain. This operation requires an authorized agent administration. Figure 8 shows secure communications between authentication authorities of neighboring domains in pervasive networks.

In each domain of ubiquitous network, there exist a variety of services and a multiplicity of users. The user authenticated and authorized by the authority of the domain, of which he belongs, can reach the services of his domain.

We can formalize by $U_{iA}$ the user i of the domain A and by $S_{jA}$ the service j provided in the domain A. thereby, the user $U_{iA}$ $\forall$ i $\in$ {1, N} can access to service $S_{jA}$ $\forall$ j $\in$ {1, M} if he is authenticated by RA and authorized by CA in the domain A.

The basic security protocol is extended for inter-domains authentication in our proposal. Taking an example, the users $U_{iA}$ with access to servers $S_{jA}$ can also access services (S1, S2, . . . , SM) in the other network

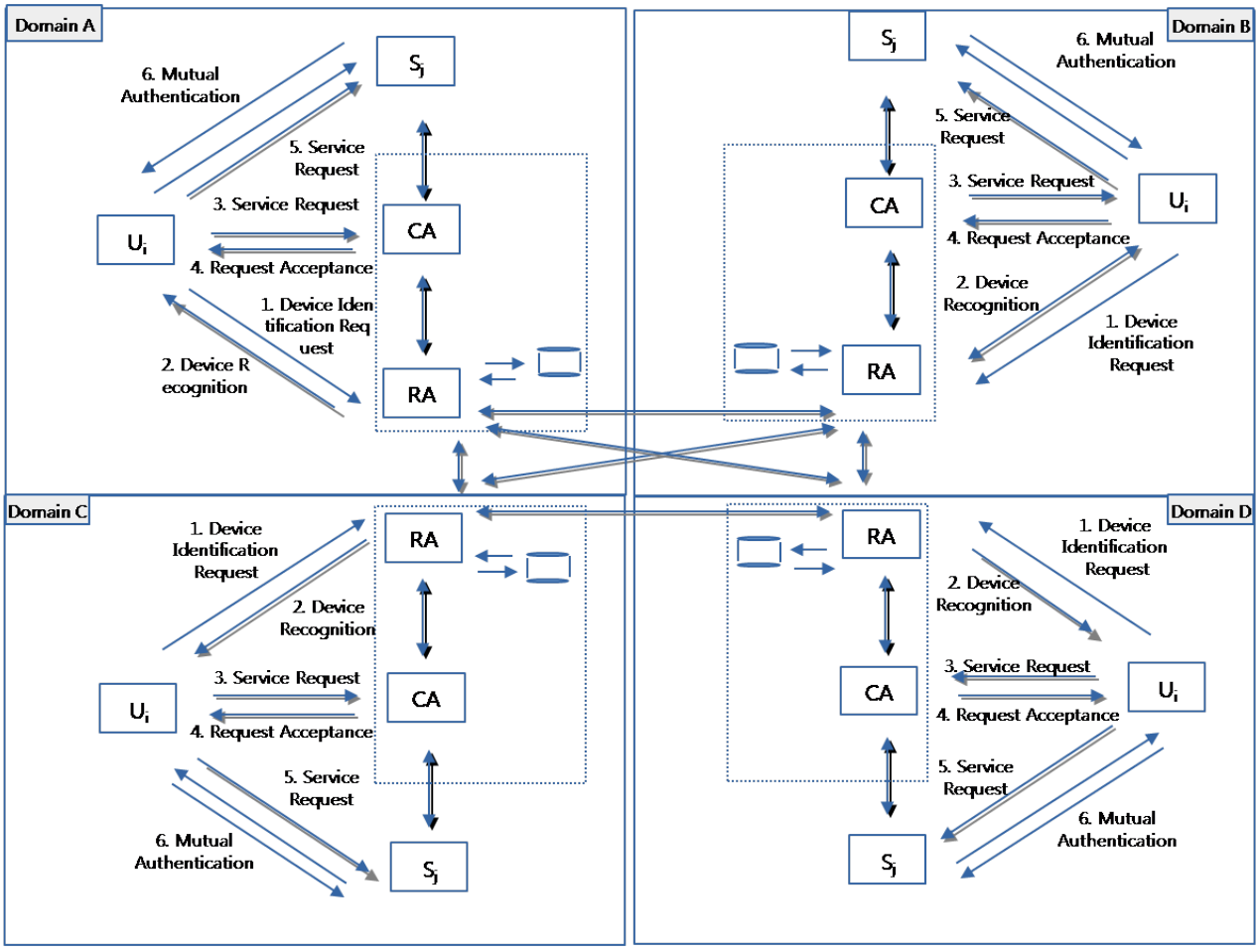


Fig. 8. Process of inter-domain connection.

domains (B, C, D). The users $U_{iA}$ ∀ i Є {1, N} can access to services $S_{jd}$ ∀ j Є {1, M} and ∀ d Є {A, B, C, D} being authenticated by RA and authorized by CA in the domain A.

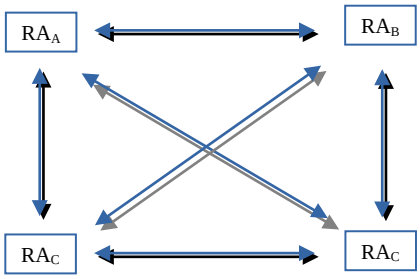


Fig. 9. Inter-domain connection with direct communication between Registration Authorities

For example, the user $U_{iA}$ has been authenticated by RA and authorized by CA in the domain A. So, to access to services in domain B, $U_{iA}$ sends a request to CA in the domain B. CAB consults RAB who checks the registration of $U_{iA}$ initially in the domain B and in the surrounding domains in two distinct ways: •

• In the first infrastructure, RAB launches an identification request of $U_{iA}$ to neighboring RAd ∀ d Є {A, C, D}. RAA recognizes the user $U_{iA}$ and answers by assertion by sending the necessary information concerning $U_{iA}$. RAB accepts the authentication sent by RAA and CAB can authorize $U_{iA}$ to access to services in the domain B.

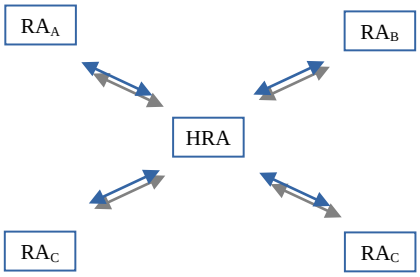


Fig. 10. Inter-domain connection with Hierarchical central Registration Authorities.

Inter-domain authentication requires two RA belonging to both network domains to have a path of trust established from one network domain to another domain, and they must have agreed secret keys, in network domain A and B respectively. It is vital to note that remote network domain trusts the RAA of the local domain as the remote RAd d Є {B,C,D} do not carry out their own authentication check of the visiting users $RA_{iA}$. Thus, with our proposed security protocol for ubiquitous network access, we could achieve computationally fast and uniform. Figure 9 illustrates the extension proposal of the above basic security protocol for inter-domain communications with direct communication between RA.

• In the second infrastructure, a central hierarchical registration authority HRA connects the registration authorities of different neighboring domains and plays intermediary's role and sometimes a hierarchic authority.

In the previous example, RAB launches an identification request of $U_{iA}$ to HRA. HRA sends this request to RAD ∀ d Є {A, C, D} which comes under its authority. RAA recognizes the user $U_{iA}$ and answers to HRA by assertion by sending the necessary information concerning $U_{iA}$. In turn, HRA answers to RAB which accepts the authentication sent by RAA to HRA and CAB can authorize $U_{iA}$ to access to services in the domain B.

In this infrastructure inter-domain, HRA connects different RA of different domains. Inter-domain authentication requires to have a path of trust established from every network domain to HRA, and a secret keys agreement must be established between HRA and every network domain $RA_d$ ∀ d Є {A, B, C, D}. Figure 10 illustrates the extension proposal of the above basic security protocol for inter-domain communications with a central hierarchical RA.

Table 4. Notations used in the proposed scheme.

| Symbol | Definition |
|---|---|
| $U_i$ | User i |
| $ID_i$ | User's identity |
| $TID_i$ | Transformed identity of $U_i$ |
| $PW_i$ | User's chosen password |
| $TPW_i$ | Transformed password of $U_i$ |
| $\beta_i$ | Biometric information |
| RA | Authentication Authority |
| CA | Authorization Authority |
| $SN_j$ | Service node i |
| $SID_i$ | Service Identifier |
| $TS_k$ | Service Type k |
| $S_{RUi}$ | Secret key of RA for $U_i$ |
| $S_{RC}$ | Common Secret between RA and CA |
| $S_{Sk}$ | Service Type secret |
| h(.) | One-way hash function |
| ⊕ | An XOR operation |
| \|\| | String concatenation |

The HRA must be a trusted party in our inter-domain device authentication system. HRA is a coordinator between the various authorities of various domains. It allows the system to maintain the knowledge of users authenticated at least once and travelling between network domains. HRA will also play the role of a central

registration authority such as a PKI-based device authentication mechanism. In this infrastructure, the device authentication framework has a hierarchical PKI structure [34, 40, and 41]. That is, a HRA manages domain registration authority (RA) and RA controls domain users and services devices. The RA is a domain device with sufficient computing power for public key operation and for communication with other domain devices and user interface equipment. The RA, which also functions as a regular registration authority (RA) has more authority and requirements. To note that various domain devices connected to the network can communicate with each other and have basic computing ability, including the following: an Internet-microwave, an Internet-refrigerator, a digital TV such as IPTV, an Internet-washing machine, a PDA, a notebook computer, a wall-pad, a PC, and a cellular phone. Many devices are used in everyday life and more will soon be developed [42, 43].

**2. Security Protocol**

Generally, a PCE consists of three types of entities: mobile users, services and back end authentication servers, in addition to the underlying wired and wireless communication infrastructures.

Our proposed access control scheme is designed to secure the interactions among these three types of entities, i.e., the smart user, the smart service and the gateway composed of two entities, i.e., authentication and authorization authorities. The notations and their corresponding definitions are listed in table 4.

The access process of a user to the pervasive network services in figure 11 is described as follows:

**1) Registration Phase**

In this section, we propose a biometric user authentication scheme which wraps mutual authentication and user anonymity. The proposed scheme is composed of four phases: registration, login, authentication and password changing. When an offer comes into service or a user Ui wants to access a smart server for a legitimately service, SNj and Ui should perform the following registration steps:

**Smart service registration**

**Step 1.** $SNj \Rightarrow CA : <SID_j, TS_k>$

Every smart service $SN_j$ provided in the pervasive network registers his service in the authorization authority by transmitting the identity $SID_j$ and the service type provided $TS_k$.

**Step 2.** $CA \Rightarrow SN_j : <S_{SK}>$

Authentication authority Stores $<SID_j, TS_K>$ and transmits the secret service type $S_{SK}$ to the smart service.

**Smart user registration**

**Step 1**. $U_i \Rightarrow PA : <ID_i, PW_i , \beta_i>$

Ui chooses his identity IDi, his password Pwi, inputs his personal biometric βi on the specific device and presents them to the authentication authority in person.

**Step 2**. $RA \Rightarrow U_i : <S_{RUi}, h(.)>$

The authentication authority performs the following steps :

1. Generate transform identity $TID_i = h(ID_i \| SRU_i)$ where $S_{RU}$ is a secret key of RA for $U_i$.
2. Generate transform password TPWi= h(PWi || SRUi)
3. Compute $Fi = h(\beta_i)$

4. Store $< TID_i , TPW_i , F_i , S_{RUi}>$

**2) Login and Authentication Phase**

After the user $U_i$ registers to authentication authority RA, when $U_i$ wants to log into network service $SN_j$, $U_i$ will send a login request to RA. After user identification success, the user must send a request for particular service $TS_k$ to authorization authority CA. Once the request is accepted, a mutual authentication is lunched between smart network service $SN_j$ and smart device or user $U_i$. With transformed identity and password in the login message, the scheme proposed guarantees user anonymity and provides mutual authentication. The login and the authentication mechanisms work as follows:

a) Login Phase

**Step 1**. $Ui \Rightarrow RA : <TID_i,F_i>$

When Ui wants to log in to the system,

1. Input first identity $ID_i$ and compute $TID_i=h(ID_i||S_{RU})$
2. Input personal biometric βi on the specific device and compute $F_i = h(\beta_i)$.
3. Send $<TID_i,F_i>$ to CA

**Step 2**. $RA \Rightarrow U_i : <M_1>$

RA verifies $TID_i$ and $F_i$. If the identity information is recognized, RA performs the following operations:

1. Compute $e_i = h(TID_i \| S_{RC})$ where SRC is a common secret key between RA and CA.
2. Compute $M1 = e_i \oplus h(TPW_i \| F_i)$
3. Send <M1> to $U_i$

**Step 3**. $U_i \Rightarrow RA : <TID_i, M_3, TS_k>$

$U_i$ inputs $PW_i$ and proceeds with the following operations:

1. Compute $TPW_i = h(PW_i \| SRU_i)$
2. Compute $M_2 = M_1 \oplus h(TPW_i \| F_i)$
3. Generate $x_i$
4. Compute $M_3 = M_2 \oplus x_i$

5. Send <$TID_i$, $M_3$, $TS_k$> to CA

**Step 4**. CA $\Rightarrow$ $U_i$ : <$M_5$,$M_6$> ; CA $\Rightarrow$ $SN_j$ : <$TID_i$,$M_3$>
CA computes sequentially $M_4 = M_3 \oplus h(TID_i \| S_{RC})$, $M_5 = h(TID_i \| S_{Sk}) \oplus M_4$, $M_6 = h(M_3 \| M_4)$ and sends <$M_5$,$M_6$> to $U_i$ and <$TID_i$,$M_3$> to $SN_j$

b) Authentication Phase:

**Step 1**. $U_i \Rightarrow SN_j$ : <$TID_i$,$M_7$>
$U_i$ checks if $M_6$ =? $h(M_3 \| x_i)$. In the positive case, $U_i$ generates $y_i$, computes $M_7 = M_5 \oplus x_i \oplus y_i$ and send <$TID_i$,$M_7$> to $SN_j$.

**Step 2**. $SN_j \Rightarrow U_i$ : <$M_9$,$M_{10}$>
$SN_j$ computes $M_8 = M_7 \oplus h(TID_i \| S_{Sk})$, generates $z_i$, computes $M_9 = h(M_3 \oplus y_i) \oplus z_i$, $M_{10} = h(M_7 \| M_8)$ and sends <$M_9$,$M_{10}$> to $U_i$.

**Step 3**. $U_i \Rightarrow SN_j$ : <$M_{12}$>
$U_i$ verifies if $M_{10}$ =? $h(M_7 \| y_i)$. In the favourable case, $U_i$ computes $M_{11} = h(M_3 \oplus y_i) \oplus M_9$, $M_{12} = h(y_i \| M_{11})$ and sends <$M_{12}$> to $SN_j$ .

**Step 4**.
$SN_j$ verifies if $M_{12}$ =? $h(M_7 \| M_8)$ then $SN_j$ authenticates $U_i$ and $U_i$ authenticates $SN_j$.

**3) Identity-Changing Phase**

When $U_i$ wants to change personal information, he sends in secure channel his old information $ID_i$, $PW_i$, $\beta_i$ and new $ID_i$*, $Pw_i$* to RA. Once the change request is received by the authentication authority, RA proceeds by:

1. Compute $TID_i = h(ID_i \| SRU_i)$,
   $TPW_i = h(PW_i \| SRU_i)$ and $F_i = h(\beta_i)$
2. Verifies $TID_i$ and $F_i$
3. Compute $TID_i = TID_i \oplus h(ID_i^* \| SRU_i)$, $TPW_i = TPW_i \oplus h(PW_i^* \| SRU_i)$
4. Replace $TID_i$ with $TID_i$* and $TPW_i$ with $TPW_i$*

## VI. SECURITY PROTOCOL EVALUATION

With Remote access control, users are allowed to remotely access and control pervasive appliances such as TV, light, washing machine, audio system, PC, laptop, mobile device. This important service can cause serious security vulnerabilities to the pervasive network. To do this, it has become essential to design and implement software and hardware infrastructure to strengthen security in the PCE.

A legitimate user must pass through 3 phases of recognition: authentication, authorization and service access. Authentication entity verifies the identity of the device and particularly the user like Registration Authority in PKI. An authenticated device receives a codified message which only authorization entity can decode in the access authorization request to service submitted by the device. The authorization entity trusts the information in the request because the authentication entity already verified it. But, it restricts the access right to service. An authorized device received a codified message which only smart server can decode in the final mutual authentication between smart service and smart device. This authentication and authorization process on 3-step will protect the network services, the users privacy and unmasks any adversary attempting fraudulent access by replication or alteration of messages addressed previously to authenticated users.

**1. Security Analysis**

• An attack trying to derive secret from intercepted messages, is computationally infeasible because of the property of the one-way hashing function and random values.

• The information secret transmitted to user or smart service in the registration phase can be stored in electronic puce or smart card which if it's lost, it is difficult for any adversary to derive information

• The biometric identification allows thwarting any fraudulent attempt. A user or an adversary who enters the field of pervasive network is automatically identified by fingerprint reader, speech/pattern recognition expert device. He cannot deceive the entity authentication by a fraudulent login or the authorization entity to access a particular service. In addition, replication or modification of intercepted message proves ineffective, since he does not hold the secrets ($S_{RC}$, $S_{sk}$) and nested random values ($x_i$, $y_i$, $z_i$). Finally, mutual authentication between adversary and smart service thwarts the attempt because he fails to decrypt the message sent.

The security protocol model for ubiquitous networks proposed in this paper is able to fully satisfy the security requirements of Ambient Networks [1, 2]. The authentication mechanism is computationally fast. The model is able to prevent password guessing techniques by implementing biometrics data with password protections. The proposed security protocol model prevents passive and active attackers who impersonate other identities when accessing ubiquitous services.

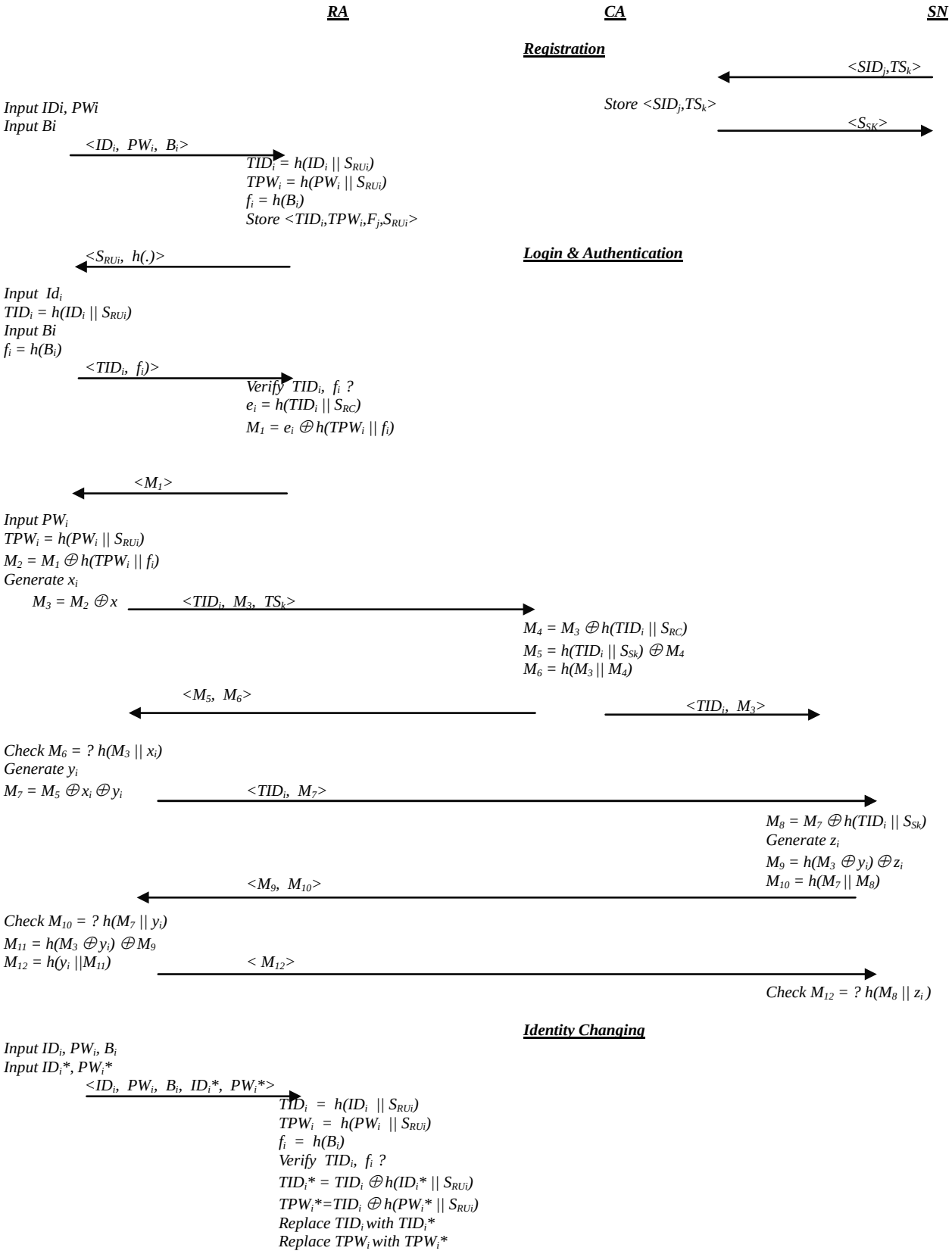


Fig. 11. The proposed scheme

**2. Performance Analysis**

The Involved parties need only lightweight cryptographic operations which reduce the computational cost. They need only a few hashing function and do not require any exponential operation which in terms of efficiency is very high-powered and time-consuming.

In term of performance, the computation costs in Lin and Lai's [8] scheme are very low, only a few hashing function computations are needed. Khan et al. [7], Li and Hwang [11], Wang et al. [48] and Vaidya et al. [45] schemes present a little more cost of treatment. Our scheme is in the middle of presented schemes in term of cost of treatment. This is due in one side that certain presented schemes realize a direct authentication between user and server without an intermediary authority and in other side, other schemes realize authentication with a single level of authentication. Our scheme presents authentication in two levels; the first one allows users registration and authentication by registration authority and in the second, authorization authority gives users authorization to access to services provided by the system. This idea may be more appropriate to pervasive computing environments: The environment which was not considered by the other schemes. The Lin and Lai's [8], Khan et al. [7] and Li and Hwang [11] schemes developed a biometric authentication. Our scheme puts into practice the biometric authentication idea of Li and Hwang [11] for pervasive computing environment. However, the Tseng et al. [47], Wang et al. [48] and Shin et al. [49] schemes developed an ID-based or password-based remote user authentication without intermediary authority between user and server. Ko [44], Vaidya et al. [45] and Xue et al. [46] schemes developed an ID-based or password-based authentication for wireless sensor network. We can add that among authentication those which are with smart-card based in user side.

To note that Lin and Lai's [8], Tseng et al. [47] and Shin et al. [49] schemes require some exponential operations because the security of the schemes is based on solving discrete logarithm problems. But, the exponentiation operations might be expensive. Its use is sometimes motivated by the increasing demand for information security and the research of more secure authentications by complicated computations which will be widely adopted as a necessary security measure. However, we consider that exponentiation operation might be expensive for small and off limited power and computation capacity device and in terms of efficiency; the exponential computation is very high-powered and time-consuming.

**3. Functionality Analysis**

The scheme allows users to freely choose the initial passwords during the registration phase and provides the functionality of identity changing. The scheme provides mutual authentication, achieves non-repudiation by employing personal biometrics and does not require synchronized clocks by use of random numbers.

Table 5. Performance analysis of authentication schemes

| | Registration | Login & Authentication | Total |
|---|---|---|---|
| Khan et al. [7] | 2H | 7H | 9H |
| Lin and Lai [8] | 1H, 1E | 3H, 4E | 4H, 5E |
| Li and Hwang [11] | 3H | 7H | 10H |
| Ko [44] | 2 H | 14H | 16H |
| Vaidya et al. [45] | 4H | 9H | 13H |
| Xue et al. [46] | 12H | 27H | 39H |
| Tseng et al. [47] | 5H | 10H, 2E | 15H,2E |
| Wang et al. [48] | 2H | 6H | 8H |
| Shin et al. [49] | 3H, 1E | 8H,1E | 11H,2E |
| Our scheme | 3H | 13H | 16H |

Table 6. Functionality analysis of authentication schemes.

| | Password Changing | Mutual Authentication | Without time synchronization | User Anonymity |
|---|---|---|---|---|
| Khan et al. [7] | Yes | Yes | No | No |
| Lin and Lai [8] | Yes | No | No | No |
| Li and Hwang [11] | Yes | Yes | Yes | No |
| Ko [44] | Yes | Yes | No | No |
| Vaidya et al. [45] | Yes | Yes | No | Yes |
| Xue et al. [46] | Yes | Yes | No | Yes |
| Tseng et al. [47] | Yes | Yes | No | Yes |
| Wang et al. [48] | No | Yes | No | No |
| Shin et al. [49] | Yes | Yes | Yes | Yes |
| Our scheme | Yes | Yes | Yes | Yes |

Except for Wang et al. [48] scheme, the majority of presented schemes allow a free choice of password or its change. Also, except for Lin and Lai's [8] scheme, all the schemes provide mutual authentication between the two communication parties.

On the other hand, an important number of schemes required synchronized clocks between the user and the remote server because of using timestamps. In fact, it is fairly complicated to achieve time concurrency and some disadvantages exist such as the delivery latency and the different time zone. Li and Hwang [11], Shin et al. [49] and our schemes do not require synchronized clocks by the use of random numbers in place of timestamps.

Not forget to underline that by the application of the personal biometrics, the authentications by biometric recognition achieve non-repudiation.

The proposed authentication in this paper is pertinent to using in pervasive computing environment. In addition, the proposed scheme achieves mutual authentication in an anonymous way.

## VII. CONCLUSION

In order to make human life more convenient, the rapidity of the development on electronic technology made it possible to implement various mobile devices with different capabilities and different usage. This progress has enriched communication park but led to an implementation of object of all-out. In this technology Bazaar where servers propose more offer, users demand more service, designers and administrators provide more effort for preservation of user's privacy, protection of services access and communications between stakeholders in this context. So, in an environment where by default each object will be connected and accessible, arise necessarily issues of confidentiality, privacy and non-intrusion. For that, it has become essential to implement infrastructures which secure the network and offer a pleasant ubiquitous setting. Over a wireless and/or wired network infrastructure, a PCE consists of three types of entities: mobile users, services and back end authentication servers. To make the system architecture more scalable and flexible, a broker can be introduced between the user and service. Both users and services can interact with brokers to subscribe and distribute services.

In this paper, we discussed an access control scheme which aimed to secure the interactions among component entities of PCE. By a user privacy preserving authentication, it addressed the security and user privacy concerns in PCEs. The proposed security system is based on an infrastructure consisting of authority by domain. By modular composition, each authority is composed of entity of user's authentication and entity of authorization for authenticated users to the services provided by the pervasive network. The proposed scheme provides explicit mutual authentication between concerned parties while at the same time allowing the mobile user to interact with the desired service anonymously without revealing its identity. Up to now, it is difficult to definitely decide which mechanism is suitable for pervasive network. Authentication in a pervasive system can be based on one of the varieties of authentication namely ID-password-based authentication, certificate-based authentication or biometric information-based authentication. But, since biometric keys are based on physiological and behavioral characteristics of persons, Biometric information-based authentication reveals very promising and reliable.

## VIII. FURTHER RESEARCH

Our current researches turn around the pervasive computing environment security and the preservation of the user's privacy and intimacy. At present, we manage to achieve the users privacy by realizing two of the relatives principles namely sovereignty and minimization of the data. For the storage of biometric templates, each location has advantages and weaknesses in terms of processing time, confidentiality and privacy respect. To note that in France, the National Commission of data processing and freedoms (CNIL) prohibits the use of the centralized basis for a large number of individuals. So, the realization of the first principle, namely the data sensibility, requires a decentralized structure for data storage. For that purpose, our next researches steps will tend to decentralize the ubiquitous networks security. Basing on the foundations of the distribution systems, we can develop this idea. This challenge will can, if we manage to concretize it, relieve the constraints of the bottleneck from which suffer objects brought to follow a local security strategy in networks generally and in ubiquitous environment particularly. In a word, despite the efficiency provided by a centralized security solution, it makes lose to the entities belonging to the network their ubiquitous character.

REFERENCES

[1] Ambient networks project, http://www.ambient-networks.org/.

[2] Wireless world initiative, http://www.wireless-world-initiative.org/.

[3] R. Haladjian, “De l’inéluctabilité du réseau pervasif,” *FING*, 2004.

[4] M. Satyanarayanan, “Pervasive computing: Vision and challenges,” *in Proceedings of the IEEE Personal Communications*, August 2001.

[5] F. Stajano, *Security for Ubiquitous Computing*. John Wiley and Sons Inc., February 2002.

[6] M.K. Khan, J. Zhang, "Improving the security of a flexible biometrics remote user authentication scheme," *Computer Standards and Interfaces*, Vol. 29, No. 1, pp. 82–5, 2007.

[7] M.K. Khan, J. Zhang, X. Wang, "Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices," *Chaos, Solutions and Fractals*, Vol. 35, No. 3, pp. 519–24, 2008.

[8] C.H. Lin, Y.Y. Lai, "A flexible biometrics remote user authentication scheme," Computer Standards and Interfaces, pp. 19–23, 27(1), 2004.

[9] J.K. Lee, S.R. Ryu, K.Y. Yoo, "Fingerprint-based remote user authentication scheme using smart cards," *Electronic Letters*, Vol. 38, No. 12, pp. 554–5, 2002.

[10] B.T. Hsieh, H.Y. Yeh, H.M. Sun, C.T. Lin. "Cryptanalysis of a fingerprint-based remote user authentication scheme using smart cards," *In Proceedings of 37th IEEE conference on security technology*, pp. 349–50, 2003.

[11] C.T. Li, M.S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," *Journal of Network and Computer Applications*, Vol. 33, pp. 1–5, 2010.

[12] Weiser M., *The Computer for the Twenty-First Century*. Scientific American, September, pp 94-10, 1991.

[13] S. S. H. Naqvi, "Architecture de Sécurité pour les Grands Systèmes, Ouverts, Répartis et Hétérogènes," Thesis, Higher National School of Telecommunication, Paris, France, December 2005.

[14] C.Y. Yeun, E.K. Lua, J. Crowcroft, "Security of emerging ubiquitous networks," *proceeding of IEEE 62nd Semiannual vehicular technology conference*, Dallas, Texas, USA, Vol 2, pp. 1242-1248, September, 2005.

[15] A. Abdul-Rahman, S. Hailes, "Supporting trust in virtual communities," *in Proceedings of the IEEE Hawaii International Conference on System Sciences 3*3. IEEE, pp. 4-7 January 2000.

[16] S. Buchegger and J. Y. L. Boudec, "A robust reputation system for peer-to-peer and mobile ad-hoc networks," *in Proceedings of the P2PEcon 2004*, June 2004.

[17] "Common Criteria for Information Technology Security Evaluation," *Department of Health, July* 2009.

[18] J. Al-Muhtadi, A. Ranganathan, R. Campbell, and M. Mickunas, "A flexible, privacy-preserving authentication framework for ubiquitous computing environments," *in Proc. ICDCS Workshops*, pp. 771–776, 2002.

[19] K. Ren, W. Lou, K. Kim and R. Deng, "A Novel Privacy Preserving Authentication and Access Control Scheme for Pervasive Computing Environments", *IEEE Transactions on Vehicular Technology*, vol. 55, no. 4, pp. 1373-1384, 2006.

[20] H. Aboalsamh, F. Alanizi, M. Bin Sabbar, S. AlRabiaah, "Security in Ubiquitous Computing: A Work in Progress," the 2013 World Congress in Computer Science, Computer Engineering and Applied Computing, (WORLDCOMP 2013), *The 2013 International Conference on Wireless Network (ICWN'13)*, Las Vegas, Nevada, USA, pp. 424-430, July 2013.

[21] J. Al-Muhtadi, R. Campbell, A. Kapadia, D. Mickunas, and S. Yi, "Routing through the mist: Privacy preserving communication in ubiquitous computing," *in Proc. ICDCS*, Vienna, Austria, pp.65–74, 2002.

[22] A. Pfitzmann and M. Hansen. "Anonymity, unlinkability, unobservability, pseudonymity, and identity management - a consolidated proposal for terminology," Technical Report, v0.31, 2008.

[23] A. Plateaux, P. Lacharme, "Organisation d'une architecture de santé respectueuse de la vie privée," *7ème Conférence sur la Sécurité des Architectures Réseaux et Systèmes d'Information (SAR SSI)*, Cabourg, France, 2012.

[24] K. Markantonakis and K. Mayes, "An overview of the GlobalPlatform smart card specification," *Information Security Technical Report: Smart Card Security*, vol. 8, no. 1, pp. 17–29, 2003.

[25] V. Alimi, R. Belguechi, C. Rosenberger, "Secure and Privacy Preserving Management of Biometric Templates," *3rd Edition on the Norwegian Information Security Conference*, NISK, pp 134-146, November 2010.

[26] K. Phua et al., "Heart sound as a biometric," *Pattern Recognition*, Vol. 41, No. 3, pp.906-919, 2007.

[27] R. Palaniappan, "Electroencephalogram Signals from Imagined Activities: A Novel Biometric Identifier for a Small Population," *E. Corchado et al. (Eds.): IDEAL, LNCS 4224*, pp. 604 – 611, 2006.

[28] R. Giot, M. El-Abed, C. Rosenberger, "GREYC Keystroke: a Benchmark for Keystroke Dynamics Biometric Systems," *IEEE Third International Conference on Biometrics: Theory, Applications and*

*Systems (BTAS)*, Washington DC USA, Sept. 28-30, 2009.

[29] P.O. Ladoux, C. Rosenberger, B. Dorizzi, "Hand Vein Verification System based on SIFT matching," *The 3rd IAPR/IEEE International Conference on Biometrics (ICB)*, pp.1297–1305, 2009.

[30] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Security & Privacy*, Vol. 1, pp; 33–42, 2003.

[31] J. Mahier, M. Pasquet, C. Rosenberger, and F. Cuozzo, *Biometric authentication*, Encyclopedia of Information Science and Technology, pages 346–354, 2008.

[32] International Biometric Group. http ://www.biometricgroup.com/, 2010.

[33] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *In Proceedings of the IEEE*, vol. 91, pp. 2021–2040, 2003.

[34] M. M. El Abed, "Evaluation de sytèmes biométriques," Thesis, Université Caen/BassE-Normandie, France, December 2011

[35] ISO/IEC 19795-1, "Information technology – biometric performance testing and reporting – part 1: Principles and framework," 2006.

[36] Y. Jeong, K. Yoon, J. Ryou, "A Trusted Key Management Scheme for Digital Right Management," *ETRI Journal*, vol.27, no.1, pp. 114-117, Feb., 2005.

[37] D.G. Lee, J.W. Han, D.S. Park, I.Y. Lee, "Intelligent Pervasive Network Authentication: S/Key Based Device Authentication," *Consumer Communications and Networking Conference*, 2009.

[38] C. Gehrmann, K. Nyberg, C.J. Mitchell, "The personal CA-PKI for a personal area network," *IST Mobile and Wireless Telecommunications, Summit 2002*, pp. 31-5, 2002.

[39] J.B. Hwang, H.K. Lee, J.W. Han, "Efficient and User Friendly Inter-domain Device Authentication/Access control in Home Networks," *In Proc. 2nd International Conference on Embedded and Ubiquitous Computing*, Aug., 2006.

[40] Intermediate specification of PKI for heterogeneous roaming and distributed terminals," IST-2000-25350-SHAMAN, March, 2003.

[41] R. Housley and T. Polk, *Planning for PKI: Best Practices Guide for Developing Public Key Infrastructure*, John Wiley & Sons, Inc. 2001.

[42] Y. Lee, D. Lee, J. Han, T. Kim, "Home Network Device Authentication:Device Authentication Framework and Device Certificate Profile," *The computer Journal*, 2008.

[43] Y. K. Lee, J. W. Han, D. G. Lee, J. N. Kim, "Home Device Authentication Framework and Implementation," *International Journal of Smart Home*, Vol. 2, No. 4, October, 2008.

[44] L.C. Ko, "A novel dynamic user authentication scheme for wireless sensor networks," *Proceedings of the IEEE International Conference on (IEEE ISWCS 2008)*, Reykjavik, Iceland, pp.608–612, October 2008.

[45] B. Vaidya, J.J. Rodrigues, J.H. Park, "User authentication schemes with pseudonymity for ubiquitous sensor network in NGN," *International Journal of Communications Systems*, vol.23, pp.1201–1222, 2010.

[46] K. Xue, C. Ma, P. Hong, R. Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," *Journal of Network and Computer Applications*, vol.36, 2013.

[47] H. R. Tseng, R. H. Jan, W. Yang, ″A bilateral remote user authentication scheme that preserves user anonymity,″ *Journal of Security and Communication Networks*, Vol. 1, No. 4, pp. 301-308, Jul/Aug, 2008.

[48] Y. Y. Wang, J. Y Kiu, F. X. Xiao, and J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme," *Computer Communication*, vol. 32, pp.583–585, 2009.

[49] S. Shin, K. Kim, K. H. Kim, and H. Yeh, "A Remote User Authentication Scheme with Anonymity for Mobile Devices", *International Journal of Advanced Robotic Systems*, Vol. 9, pp. 1-7, 2012.

## Authors

**Pascal Lorenz** (lorenz@ieee.org) received his M.Sc. (1990) and Ph.D. (1994) from the University of Nancy, France. Between 1990 and 1995 he was a research engineer at WorldFIP Europe and at Alcatel-Alsthom. He is a professor at the University of Haute-Alsace, France, since 1995. His research interests include QoS, wireless networks and high-speed networks. He is the author/co-author of 3 books, 3 patents and 200 international publications in refereed journals and conferences. He has served as Co-Guest Editor for special issues of IEEE Communications Magazine, Networks Magazine, Wireless Communications Magazine, Telecommunications Systems and LNCS. He is senior member of the IEEE, IARIA fellow and member of many international program committees. He has organized many conferences, chaired several technical sessions and gave tutorials at major international conferences. He was IEEE ComSoc Distinguished Lecturer Tour during 2013-2014.

**Abdallah Chouarfia** is a Professor in the Department of computer sciences at University of Sciences and Technology of Oran (USTO-MB) Algeria. He received the B.E. degree in Computer science from CERI Algiers and Ph.D degree in software engineering from Paul Sabatier University Toulouse France (1983). He has more than 30 years of teaching experience. He has published more than 20 papers in International, National journals and conference proceedings. His areas of research include Software engineering and Networking include mobile ad hoc and security.

**Benchaà Djellali** received his engineer diploma in the option of software engineering in computer sciences in 1991 from the University of Sciences and Technology of Oran (USTO-MB) in Algeria. He works as an engineer in different computer sciences companies. He received his magister in 1997 from the University of Sciences and Technology of Oran (USTO-MB). He is an assistant professor in the Department of computer sciences at University of Sciences and Technology of Oran (USTO-MB) Algeria since 1999. He is a member of the Network and Telecommunication Research Group of Colmar (GRTC) at the haute Alsace University (UHA) in France since 2013. His research interests include parallel and distributed systems, operating systems, pervasive networks, stochastic process and Markov chains.

**Kheira Belarbi** received her engineer diploma in the option of software engineering in computer sciences in 2001 from the University of Sciences and Technology of Oran (USTO-MB) in Algeria. She received his magister in 2012 from the University of Sciences and Technology of Oran (USTO-MB). She is an assistant professor in the Department of Law and Commerce at the University of Mascara in Algeria since 2013. Her research interests include QoS, wireless and pervasive networks.