DESIGN AND IMPLEMENTATION OF A NOMADIC MOBILE APP TO AID MULTI-LEVEL AUTHENTICATION IN A UBIQUITOUS WORK ENVIRONMENT

Osaremwinda Omorogiuwa [1], Stella Chinyere Chiemeke [2], Juliana Ndunagu [3]

[1] Department of Computer Science & Information Technology, Igbinedion University, Okada, Edo State, Nigeria
[2] Department of Computer Science, University of Benin, Benin City, Nigeria
[3] Department of Computer Science, National Open University, Nigeria

Corresponding Author: Osaremwinda Omorogiuwa, ask4osas@iuokada.edu.ng

ABSTRACT: Users in a ubiquitous work environment desire comfortable interactions with their owned portable smart devices on daily basis, thus demanding the inclusion of their smart devices as an additional means of getting access to organizational systems in a seamless and user friendly manner. In response to these unique challenges, this paper advocates the inclusion of users' smartphone in achieving a multi-level authentication access in a ubiquitous work environment. This inclusion was achieved by formulating a model that includes combining at least one authentication method each from what the user has, what the user knows and what the user is. In addition, a mobile app called Nomadic App was developed using use case diagrams, HTML5.0, CSS and JavaScript. A justification of the multi-level authentication mechanism based on National Institute of Standard and Technology attained a level three status. The implementation of the developed Nomadic Mobile App improved the ease in including users' smartphones in theproposed multilevel authentication model.

KEYWORDS: Ubiquitous Computing, Ubiquitous work environment, Nomadic Mobile App, Multi-level Authentication, UML tools.

1. INTRODUCTION

Most access control systems entail the use of authentication process before actual access can be granted to users. Most organisations tend to use the single level authentication mechanism to achieve access control. Single level authentication implies the use of either a pseudo centric or a biometric means to verify and allow users access their roles in organization. Examples are the use of the simple password or the use of the finger print as means of authentication. The single level authentication approach has its strengths such as ease of use and low cost of implementation. The single level authentication approach is however prone to lots of errors (such as password theft, brute force attack, masquerading etc.) which could be capitalized upon to cause some security flaws. The use of the multi-level authentication approach is required to eradicate these problems associated with the single level authentication mechanism. Multi-level authentication approach entails the use of two or more means of authentication to grant access rights and privileges to users ([Gor03]).

Most organizations work environments are becoming smart and ubiquitous. Ubiquitous computing refers to a proliferation of lots of computing devices, sensors and embedded processors that will provide new functionality, offer expert and intelligent services, enhance productivity and facilitate seamless interaction with the surrounding environment and available resources. While traditional computing encompassed hardware and software entities, ubiquitous computing extends the boundaries of computing to include physical spaces, building infrastructures and the devices contained within. The aim is to transform passive static environment into interactive, dynamic and programmable spaces that are coordinated through a software infrastructure and populated with a large number of mobile users (also known as nomadic users) and devices. A ubiquitous work environment is the vision for the work environment of the future. It is leveraged upon the ubiquitous computing paradigm which supports collaborating nomadic users in a seamless way, providing work support anywhere and anytime. A ubiquitous work environment system design comprises both smart devices, services and their interfaces. A ubiquitous work environment infrastructure already exists in most work places unknown to them. However concerted efforts is required to consciously annex the benefits accruable to such environment by implementing software solutions that can be used to ease service delivery and resource sharing in a usable and secured manner. One of the most important factors in a ubiquitous work environment is a means of granting access to organization resources. Authentication is the process of positively verifying the identity of a user, device or other entity in a computer system, often as a perquisite to

allowing access to resources in the system ([Gor03]). Cotta et al. ([C+17]) expressed the growing importance of smart devices as a result demanding effective's user authentication mechanism. They argued that statement of art authentication mechanism are either vulnerable to known attacks or do not meet usability needs. To address this problem, a Nomadickey user-to-device authentication mechanism based on nomadic keyboards keys was designed. Mohammed et al., ([E+17]) expressed that smartphones are context-aware devices that provides a compelling platform for ubiquitous computing and assist users in accomplishing of their routine tasks anytime and anywhere. They proposed a framework that provides a platform for carrying out multi-class smart user authentication. Konstantinous et al. ([S+10]) developed a Nomad biometric authentication that could enhance mobile and ubiquitous person identification.

This paper advocates the use of a multi-level authentication method in a ubiquitous work environment to ease usability and security.

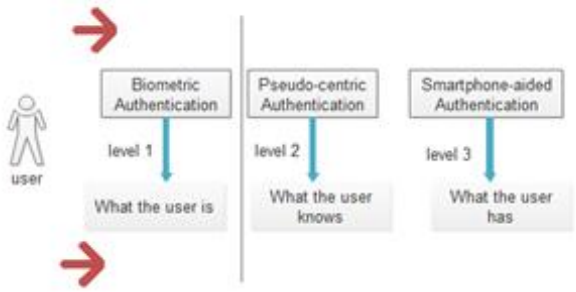

Figure 1: A Multi-level Authentication Model for a Ubiquitous Work Environment

The proposed multilevel authentication model is depicted in Figure 1 and it's explained as follows:

(i) First Level (Biometric Authentication): All users are required to carry out a one-time biometric authentication. This is used to identify the users' presence in the work environment.

(ii) Second-Level Authentication: This consists of the use of combination of password based credentials and time-stamped 4 digit randomly generated authentication passcode. The password based credentials represents the username and password while the time stamped authentication passcode is a four digit code which is required to be sent to the users smartphone via the users mobile app account.

(iii) Third-level Authentication (The Nomadic Mobile App Authentication; password- based): the Nomadic Mobile Application is a subsystem that supports the authentication module of the ubiquitous System. All users are required to provide their authentication credentials (e.g. user ID and passcode) before they can be granted access to the mobile app account. The word "Nomadic" is an acronym that stands for Network of Mobile Adaptable and Dependable Systems. A Nomadic user is therefore a mobile or stationary user that can sufficiently access organizations resources anywhere within and outside the ubiquitous work environment.

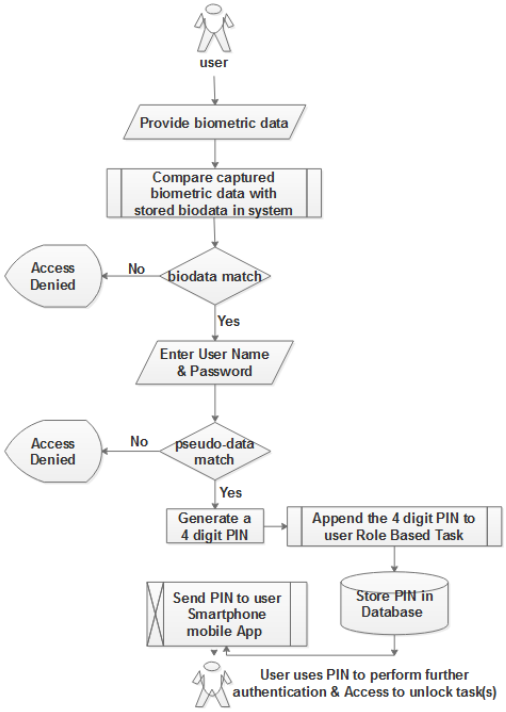

Figure 2: A process flow diagram for the Multi-level authentication Model

The process flow diagram, for the multi-level authentication model is depicted in Figure 2. It explicitly depicts the various modules and the flow of processes/events required to achieve the various levels of authentication in the ubiquitous work environment with ease in usability while still maintaining confidentiality, integrity and availability.

2. THE NOMADIC MOBILE APP ARCHITECTURE

With the advent of new smartphones and tablets and various types of media devices large flat screens, new capturing devices, and large media libraries on the other hand, new exciting smart applications are becoming increasingly popular. Cost efficient and easy to install wireless networking solutions are also important components when building applications in a ubiquitous work environment. Raihan et al. ([R+12]) proposed an architecture for nomadic mobility in smart home environments based on AAA (Authentication, Authorization and Accounting) mechanisms in conjunction with media proxies aggregating and presenting content to any type of

HTTP enabled device. However, the architecture did not support decentralized mechanism for authentication and connectivity among homes instead of relying on the central AAA node.

The Nomadic Mobile app also known as the Mobile App consist of the splash screen page, the home page with user account login prompt. At the mobile app message page, a relunch page hyperlink and logout hyperlink is displayed. The Mobile app design is based on the thin web-based client architecture. The thin client approach consists of building the business logic and data layers at the server end. The thin client is the application Graphical Users Interface (GUI).

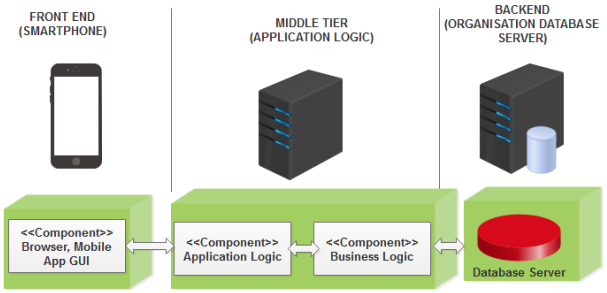

Figure 3: The Nomadic Mobile App Architecture

With this architecture in Figure 3, the smart phone user needs to be connected to the server before the application logic and the database components can be accessed. The presentation of the application logic is completely realized at the client side; only a browser in addition to the developed Nomadic App GUI is required. The server consists of the application logic which consist of a session handling component as well as components for presentation and business logic. The database is located at the server side. The browser prompts a connection to the server. Thus, the systems architecture is platform independent, it allows the cooperation with a wide range of client systems (e.g. android phones, IOS phones, Windows phones etc.) independently from the client operating systems. Furthermore, as all the data and the logic is located in the server-side, no update or synchronization mechanisms are needed. All Mobile users having the developed Nomadic mobile app installed in their mobile device can work on the same central data base, using the recent data as well as the recent presentation and business logic. The entire architecture is based on the three tier design approach. The front end is the presentation GUI of the Nomadic Mobile App, the middle layer consist of the application logic and the business logic while the backend consist of the database.

3. METHODOLOGY

A brief discussion of the UML system modelling of the Nomadic Mobile App is given as follows. First, is the use of case diagrams for the system actors (Nomadic User, client Micro browser and the Nomadic Mobile App server). The specific tools used for the modeling of the nomadic mobile app are the Use Case Diagram, Use Case Narratives and Sequence Diagrams. UML was chosen because it is a standard language for specifying, visualizing, constructing and documenting the artifacts of software systems. Also, UML represents a collection of best engineering practices that have proven successful in the modeling of complex systems. One major advantages of UML is its expressiveness as elaborated by Kendell & Kendell, ([KK07]).

Figure 4 is the use case diagram showing the system actors and use cases. The use case; request for passcode is simply required to prompt the server to perform either the Get Authentication Pin or the Delegation Passcode. The Request for Passcode use case functionality is a precondition included in both the Get Authentication and Get Delegation passcode use cases.

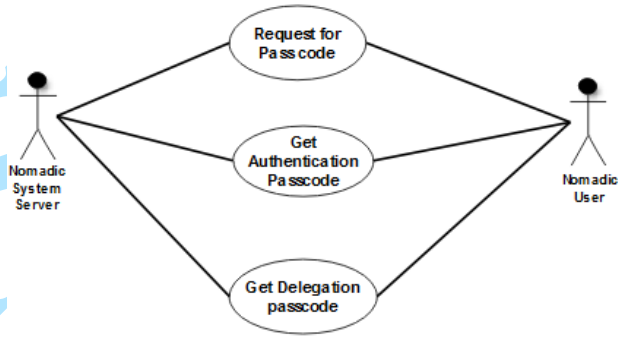

Figure 4: Use Case Diagram for the Nomadic Mobile App

The system use case narratives for each of the use cases are presented in the Tables 1 and 2.

The next figures (1 and 2) are the set of sequence diagrams use cases showing logically related sequence of event flows.

This sequence diagrams in Figure 5 and Figure 6 shows the overall pattern of activities or interactions in the use cases. The Actors and Object instances are shown in the boxes at the top of the diagrams. The leftmost object is the starting object. The top rectangles uses indicators in the name to indicate whether the rectangle represents an object, a class or an entity e.g. <<Entity>> represents the entity class System server.

Table 1: Use case Narratives to Get Authentication Passcode

Use Case 1	Get Authentication PIN
Goal in Content	All users are required to Get Pin as additional authentication credential
Level	This is the main Get Pin use case
Parameters	In: Users email, password Out: Users Sign in GUI page, Pin Sent to Users Mobile App email account
Pre-condition	Users have already be enrolled and assigned a role
Post-condition Successful Access	Authentication Passcode (Pin) generated and sent to the users Nomadic Mobile App Account
Post-condition Failed Access	Access denied; user email not in database
Actors	Users, Ubiquitous System Server
Trigger	User request to Generate Pin
Sequence of event flow	Request to Get Pin Display Generate Pin GUI page Prompt the Random Number generator to generate 4 digit Pin Add timestamp to the 4 digit Pin Store the timestamp 4 digit pin to users email account Update users database

Table 2: Use Case Narratives to Get Delegation Passcode

Use Case 2	Get Delegation Passcode
Goal in Content	All users are required to Get delegation passcode to unlock assigned task(s)
Level	This is the main Get Delegation Passcode Use case
Parameters	In: email account, passcode Out: Delegation Passcode Sent to Users email account
Pre-condition	Users have already be assigned a task or delegated a task
Post-condition Successful Access	Delegation Passcode (unlock code) generated and sent to the users Nomadic App email account
Post-condition Failed Access	Access denied; no task has being assigned or delegated
Actors	Users, Ubiquitous System Server
Trigger	User request to Generate Pin
Sequence of event flow	Request to Get Delegation Passcode Prompt the Random Number generator to generate 4 digit Pin Add timestamp to the 4 digit Pin Bind the timestamp 4 digit Pin with task-id Store the timestamp 4 digit pin to users email account Update users and task database

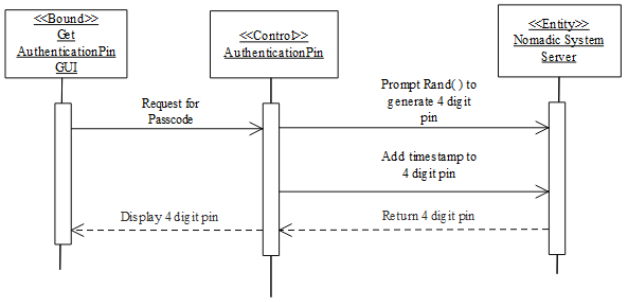

Figure 5: Sequence diagram to Get Authentication Pin

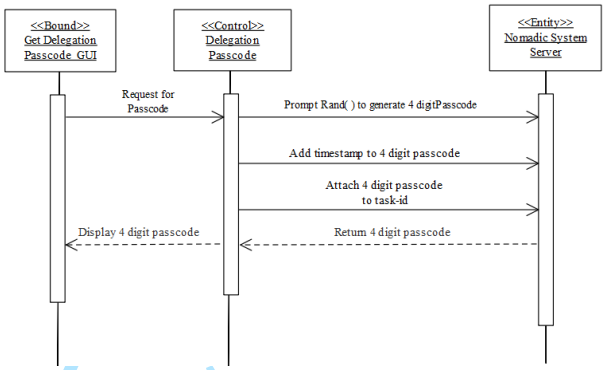

Figure 6: Sequence Diagram to Get Delegation Passcode

4. DESIGN IMPLEMENTATION

To implement multilevel authentication framework, a mobile app was developed to ease authentication process in a ubiquitous work environment. A hospital environment was used as a test case scenario as in the case with Bardram ([Bar09]). The mobile app is basically required to receive a randomly generated authentication and delegation passcode from the hospital system database server. However, the design and implementation of the hospital management system is not the focus and therefore not included in this paper. However, the focus is on the design and implementation of the nomadic mobile app. This is a core requirement to actualizing one of the research objectives of developing the1 multi-level authentication process for a ubiquitous work environment. Apache Cordova which consists of the use of HTML5.0, CSS with JavaScript was used to develop the Nomadic Mobile App software. The pseudocode required for the Biometric Authentication process required for the ubiquitous work system is represented as follows;

Pseudo code: Biometric Authentication Process

SCAN Biometric data using the fingerprint scanner

COMPARE Captured Bio metric Data with stored Bio metric Data

IF Captured Bio metric Data matches **WITH** stored Bio Metric Data

ALLOW user access **TO** System Server

ACTIVATE Get Pin generation module
ENDIF
END

The Get pin module is a randomized 64 bits encrypted number generation system. The four digit code is used as an additional information for authentication.
The 4 digit code is sent to the user mobile app account. The user logon to his mobile app account using his mobile phone. Prior to this, it is expected that the user has installed the mobile app in his smart phone. The user logon into its mobile app account using his logon credentials and gain access to the authentication and delegation passcode sent.
Both the authentication and delegation passcode are time stamped. The randomly generated authentication passcode can only be active while user is on schedule for a particular work day. After that work day, the authentication passcode becomes in-active. When a task is delegated to a user by another user, a delegation passcode is generated for that task and sent to the delegatee Mobile App account. As soon as the delegatee uses that delegatee passcode to unlock the delegated task, the Mobile App server fetches the delegation passcode from the users account (It is automatically erased from the users Mobile app account immediately the user key in the unlock task code correctly).

5. IMPLEMENTATION-TEST SCENERIO

The Hospital Management System was used to illustrate the Multi-level authentication process. Figure 7 is the first level authentication process. It consist of use of the Fingerprint scanner to gain access to the Hospital Management System (Biometric Authentication). If the biometric authentication process is successful, then the user can now have access the Hospital Management System Home page.

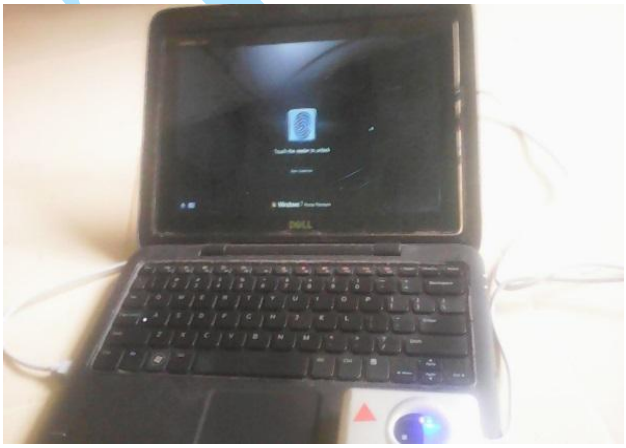

Figure 7: Screenshot of Biometric Authentication Using the Fingerprint Scanner

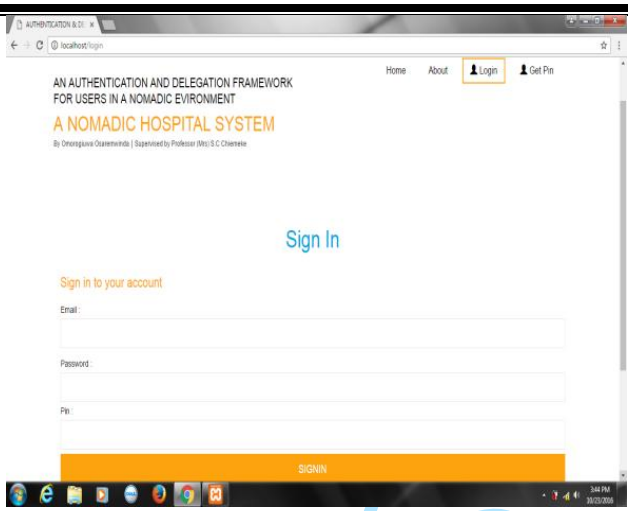

Figure 8: Screenshot Pseudo-centric Authentication Process (User of Password)

Figure 8 illustrates the use of pseudo-centric authentication process, the use of passwords (second level authentication). All users are expected to key in their username and password as a means of authentication.

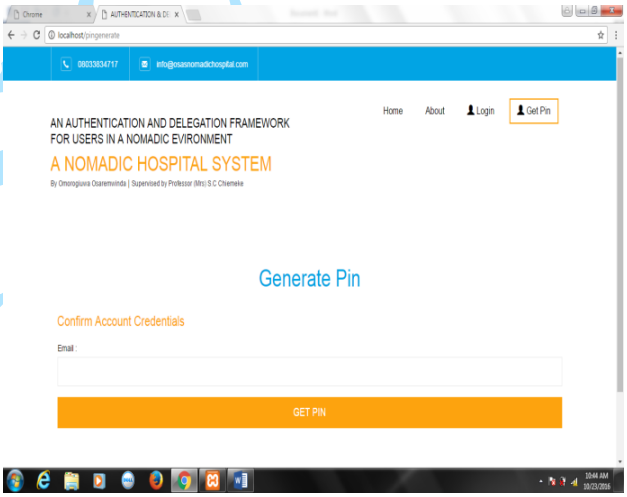

Figure 9: Screenshot of the Generate Pin (This is required to further send authentication and delegation passcodes to user smartphone

Figure 9 illustrates further the multi-level authentication process. First, the user clicks on the Get Pin. This will generate authentication passcode which is sent to the users Nomadic mobile app account installed in his smartphone shown in Figure 10. If a task is equally delegated to the user, the delegatee will equally get a delegation passcode from the delegator into its Nomadic Mobile App installed in his smartphone as shown in Figure 10.

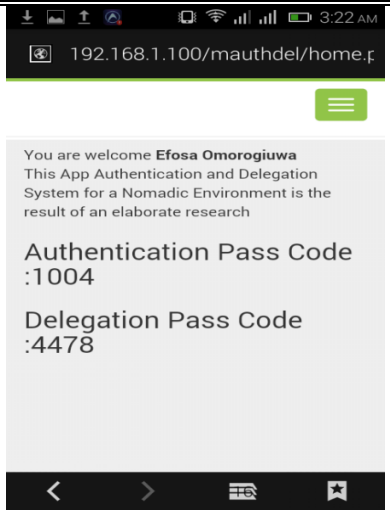

Figure 10: Nomadic User Mobile App Account Receiving Authentication and Delegation Passcodes

6. JUSTIFICATION FOR MULTI-LEVEL AUTHENTICATION PROCESS

Based on the National Institute of Standard and Technology (NIST), a special publication on Electronic Authentication Guideline ([***13]), an evaluation of the proposed multi-level authentication mechanism to ascertain level of its implementation was performed. According to NIST, the highest level is 4. In level 1, users provide the use of simple password or secret. Level 2 provides single factor remote network authentication. A wide range of authentication technologies can be employed such as single factor authentication, memorized token, out of band token, the use of biometrics and the use of single-factor One Time Password devices. Level 3 provides multi-factor remote network authentication. At least, two authentication factors are required. Level 4 is intended to provide the highest practical remote network authentication assurance. It is based on proof of possession. At this level, only "hard" cryptographic tokens are allowed. In the multi-level authentication process, we implemented the simple password based authentication (level1), the token based and biometric authentication process (level 2) and the multi-factor authentication mechanism which consist of the user ID, password and the authentication passcode sent to users smartphone through the developed Nomadic Mobile App (Level 3).

7. CONCLUSION

A multi-level authentication model for a ubiquitous work environment was implemented. The inclusion of users' smartphones during the authentication process of getting access to tasks in their work environment was achieved by developing the Nomadic Mobile App. This greatly improved the usability of the authentication model in a secured and friendly manner. The overall system implementation attained a level three standard according to National Institute of Standards.

REFERENCES

[Bar09] **Bardram J. E.** – *Activity-based computing for medical work in hospitals*. ACMTrans. Comput.-Hum. Interact. 16, 2, Article 10, 36 pages. htttp://doi.acm.org/10.1145/1534903.1534907, 2009.

[C+17] **Cotta L., Fernandes A. L., Melo L. T. C., Saggioro L. F. Z., Martins F., Maia Neto A. L., Loureiro A. A. F., Cunha I., Oliveira L. B.** – *NomadiKey: User Authentication for Smart Devices based on Nomadic Keys*. Universidade Federal de Minas Gerais (UFMG), Belo Horizonte, MG, Brazil, 2017.

[E+17] **Ehatisham-ul-Haq M., Azam M. A., Loo J., Shuang K., Islam S., Naeem U., Amin Y.** – *Authentication of Smartphone Users Based on Activity Recognition and Mobile Sensing*, Sensors, 17, 2043, 1-31, 2017.

[Gor03] **Gorman L.** – *Comparing Passwords, Tokens, and Biometrics for User Authentication*, Proceedings of the IEEE vol. 91 (12), 2019-2040, 2003.

[KK07] **Kendall K. E., Kendell J. E.** – *Systems analysis and design*, Prentice-Hall, 7th edition, 2007.

[R+12] **Raihan I., Schmidt M., Kolbe H. J., Andersson K.** – *Nomadic Mobility between Smart Homes*, Proc. of 2012 IEEE Globecom 2012 Workshops (GC Wkshps'12), Anaheim, California, USA IEEE, 1062–1067, December 2012.

[S+10] **Siriantzis K., Howells G., Deravi F., Hogue S., Radu P., McConnon G., Savatier X., Ertaud J. Y., Ragot N., Dupuis Y., Iraqui A.** – *Nomad Biometric Authentication: Towards Mobile and Ubiquitous Person Identification.* Fourth International Conference on Emerging Security Technologies, IEEE Computer Society, 1-6, 2010.

[***13] *** - *Electronic Authentication Guideline*, http://dx.doi.org/10.6028/NIST.SP.800-63-2, 2013.