Security, User Experience, Acceptability Attributes for the Integration of Physical and Virtual Identity Access Management Systems

Sara Jeza Alotaibi
Web and Internet Science
University of Southampton
Southampton, UK
sja2g09@soton.ac.uk

Mike Wald
Web and Internet Science
University of Southampton
Southampton, UK
mw@soton.ac.uk

Abstract— **A number of systems have been developed in the recent history to provide physical and virtual identity management systems; however, most have not been very successful. Furthermore, alongside increasing the level of awareness for the need to deploy interoperable physical and virtual identity management systems, there exists an immediate need for the establishment of clear standards and guidelines for the successful integration of the two mediums. The importance and motivation for the integration of the two mediums is discussed in this paper with respect to three perspectives: Security, which includes identity; User Experience, comprising Usability; and Acceptability, containing Accessibility. Not many systems abide by such guidelines for all of these perspectives; thus, our proposed system (UbIAMS) aims to change this and provide its users with access to their services from any identity access management system rather than merely providing access to a specific set of systems.**

Keywords- Physical and Virtual Identity Access Management Systems; Security; User Experience; Acceptability.

I. INTRODUCTION

The integration of physical and virtual identity access management systems has been gaining attention in different walks of life: for example, business and government agencies . Steinfield denotes the emergence of the internet as the 'death of distance', which has provoked the interoperability of the virtual and physical world[1]. He also highlights the importance of the integration of both the mediums owing to the realisation of the benefits that are: Lowering costs; Enhanced level of trust; Provision of value-added services and Access to extended segment of users.

Integration enables the provision of a centralised identity management solution with the capacity to manage the identification of users rather than the exposure of information at multiple sources and communication links[8]. Alongside the impact on the individual, effect is also felt by society. The integration of virtual and physical spaces has introduced more security for organisations since machine-readable cards are more authentic than the conventional forms of identification. The UN's International Civil Aviation Organisation (ICAO) Document 9303 provoked the emergence of e-ID cards and the integration of physical and virtual services in the UK to address the legal and political pressures of introducing such a mode of authentication[9]. The sectors will experience a lesser number of attempts to gain access by means of unauthentic modes of identification, and there should be a decreased level of identity theft and credit card fraud within society.

As stated earlier from the report by Steinfield[1], another source of motivation is that value-added services can be provided to users in the presence of the integration of the two spaces, which might not have been possible in the isolation of a physical medium: for example, conventions, helpfulness, etc. Chhanabhai states that the presence of usability makes users engage with the objects in the system, and therefore makes operations easier for them[2]. It is owing to such reasons of engagement that usability has been given due importance in the development of the proposed system. Many usability studies conclude that the usability rate of most websites is around 78%[7]; the author of the report analysed the figures and states that this figure is not adequate to facilitate the provision of a good user experience. Therefore, usability aspects need to be focused on more throughout the process of systems development.

The integration of both mediums enables access to an extended segment of users[1]. Accessibility bears great relevance in the modern world of computing; its degree of relevance can be comprehended from various examples of implementations around the world, such as Australian Government Locator Service[4], which provides a standard of nineteen factors enabling government agencies to improve the level of accessibility of their services on virtual platforms. 8% of internet users possess one or several different types of disabilities due to which conventional websites prove to be difficult for their usage[6]; amongst such users, 4% tend to have disabilities related to sight and 1% tend to have disabilities related to hearing. Astonishing figures of such a nature compel the developers to adopt measures that would improve the level of operability for all types of user, promote the inclusion of people with disabilities on a societal level, and help sectors to attract a greater number of users for their services.

This paper is organised in the following manner: firstly, a background of the relevant works and theories are clarified in

Section 2; *Section 3* proposes the **U**biquitous **I**dentity **A**ccess **M**anagement **S**ystem (UbIAMS), which is followed by a critical review and comparison of existing systems with selected criteria in *Section 4*; finally, *Section 5* ends the paper with a summary and suggestions for future work.

II. Related Works and Theories

Shibboleth is considered to be the first federated identity access management system (FIAMS) of its kind, which facilitates the transfer of users' information from one platform of security to another organisation in the same group of organisations. The emergence of this concept from Shibboleth was launched in 2003[5]. Since the emergence of FIAMSs has been witnessed only a few years ago, the level of research and development in the respective field is limited. Moreover, although several research studies have been published around the world which focus on the integration of physical and virtual services, no research study has thus far been found to include Security, User Experience and Acceptability perspectives.

A. Security and Identity

Security factors are often paid the most attention in the development of any system since its negligence can cause hefty losses for organisations; however, none of the systems that have been studied for this research possess security measures that are a nonce-based mechanism rather than timestamp[10],[11]. Furthermore, some of these systems do not provide an individual certain rights to control the exposure of his/her personal information, which thereby would enhance the overall level of privacy and security of the data[12]. Moreover, some fail to implement the concept of e-ID federation, which provides access across multiple platforms and implements a security token service (STS) based on the Windows Identity Framework[8].

B. Acceptability and Accessibility

Acceptability is the new term for 'adequate' to satisfy a need, requirement or standard, i.e. satisfactory for the user's needs, which also involves accessibility needs. There are various imperative theories that study users' acceptability and further predict the level of user intentions to utilise the system and Technology Acceptance Model (TAM) is one of them[14]. Furthermore, Pedagogy Theory revolves around the actions that impart knowledge and which are directed towards the identification of attributes that can make users' experience acceptable and accessible.[15]. Thus, the authors have formed a conceptual model based on Pedagogy Theory, learning and gaming requirements[15].

Global Interoperability Framework (GIF) has been developed on the basis of Identification, Authentication and Electronic Signature (IAS) for European countries[10],[26],[28],[29]. Secure idenTity acrOss boRders linKed (STORK) is also a project possessing the main objective of devising a framework for implementing cross-border identity management system in European countries[17]. These systems are just two examples amongst several other large projects in the chosen domain that have not concentrated on the provision of accessibility and acceptability features.

C. User Experiences and Usability

Usability is a very important factor measuring the quality of a user's experience when interacting with websites or systems. There are many organisations proposing usability theories and their components. One of the most imperative theories addresses the needs of experienced users as well as a broader set of users and technologies through introducing universal usability in relation to internet-based and other services[7],[13]. It is often witnessed that commonly discussed usability features are included in systems, whereas other features, such as conventions, mapping and cultural customisations, are not addressed. This is due to the fact that systems are commonly developed with the aim of increasing security for the user, but ultimately tend to fall short in accessibility and usability areas; therefore, the term 'user experience' is relatively newer than other domains, such as human computer interaction and usability. User Experience (UX) is an innovation and newer area of research signifying the pragmatic, useful and worthy aspects of human interaction with the computer system, alongside the viewpoint of the individual towards the realistic aspects of the system, such as helpfulness, ease of use, and efficiency.

FEderated Global Identity MAnagement framework (FEGIMA) is regarded as an effective security mechanism owing to its interoperability with different types of technologies, yet they fail to meet usability and UX requirements[18-19]. The systems are usually developed on the basis of certain types of technical expertise, whereas the altering levels of performance capabilities and disabilities are ignored.

D. Selected Attributes and Components

After conducting an extensive study concerning the available theories in the respective domain, TABLE I. shows 32 attributes which have been chosen for designing the systems of interoperable identity management systems for physical and virtual spaces;

TABLE I. Chosen Attributes for the Design

Security and Identity Attributes	
-Two factor authentication [21] -Nounce-based authentication[21] -User Anonymity [21]	-Conceal Information [16] -Security Certificates[27]. [23] -WS Federation Specification[27] -Control of information[16]
Acceptability and Accessibility Attributes	
-Incremental Learning [15] -Scaffolding [15] -Intermittent feedback[15]	-Learning Control [15] -Accommodating to the learner's style [15]
User Experiences and Usability Attributes	
-User Diversity [15] -Controllability[24] -Aesthetics [24] -Technology Variety [15] -Attitude [24] -Consistency [24], [7] -Multiple Language Support [10] -Effectiveness [24] -Efficiency [24], [25]	-Helpfulness [24] , [7], [13] -Learnability [24], [25] -Memorability [24] -Robustness [24],[7] -Simplicity [24], [7], [13] -Self-descriptiveness [24] -Perceived Affordance [24] -Mapping [24], [25] -Constraints [24]

III. PROPOSED SYSTEM

It is a common practice for government services to ask for national ID cards or biometrics for verification whilst financial institutions expect users to hold a passport or visa credit card. This practice is followed in physical spaces in prevailing times and will give the same results if the services are moved to an online platform. Owing to these limitations, a system is desired that provides interoperability between the physical and virtual spaces, alongside the option to prove one's identity with any type of identity document or biometric. There exist various systems aiming to make the physical and virtual spaces interoperable; however, none of them achieve results adequate enough to satisfy attributes from the criteria shown in Table 1. Therefore, the proposal of an innovative and original UbIAMS system will aim to incorporate all 32 attributes identified from various theories and implementations around the world.

A. Architectural Modelling

Garlan & Schmerl explain architectural modelling as various components of the system, along with the connections existing between them[30]. The architectural model for the UbIAMS is shown in Figure 1.

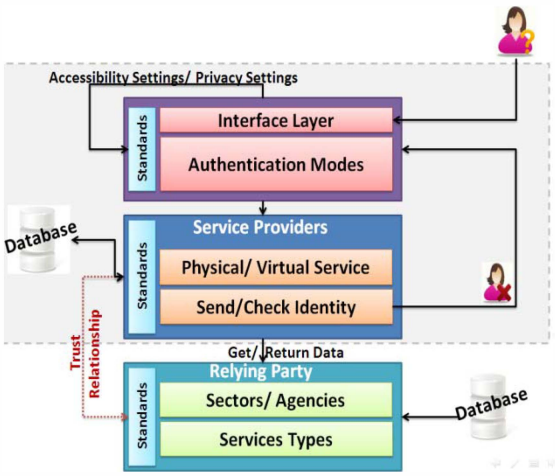

Figure 1. Architectural model of UbIAMS

It can be seen from Figure1 that there exist two layers in UbIAMS. The top layer communicates directly with the user and provides an accessible and user-friendly interface offering the choice of different authentication modes. All the functions and operations are in accordance with the standards chosen as a result of research activities in the respective domain of the study. This layer is responsible for the acquisition of the identity of the user and also for transferring the acquired information to the second layer for verification purposes.

The second layer of UbIAMS provides interoperability between the physical and virtual spaces, and thereby verifies the identity of the user with the concerned authorities. The second layer accesses the database, including information concerning the authentication modes and the different standards maintained as guiding principles for the model. Importantly, the second layer corresponds with the relying parties to verify the identity of the user with the aid of the presented authentication mode: for example, a user might present a health card, which will be used to verify the identity of the user with the hospital. The details of the user on the health card are communicated to the relying party over a secure session. Upon the successful verification of the identity of the user, the user has the benefit of availing any type of desired service ranging from financial institutions, government agencies, hospitals, etc. In the case the user is not able to provide the correct identification attributes, the user will be denied access to the services and returned back to the front layer for entry of another authentication mode.

The database located outside the layers of UbIAMS is maintained by the relying parties' therefore, the users and administrators of UbIAMS have no control over this data. With reference to the studied literature, numerous authentication modes have been identified for the proposed system. Different types of authentication modes have been classified into three categories: ownership-based factors, knowledge-based factors and inherence-based factors. Ownership-based factors include the activation of the authentication on mobile devices, smart cards and security tokens; knowledge-based factors include a secret question, PIN and passwords; inherence-based factors are further classified into physiological traits, such as fingerprints, retinal images and palm prints, and behavioural traits, such as voice, typing rhythm, and gait recognition. It can be seen from Figure 1 that standards are important aspects of the different layers within UbIAMS. The standards that have been chosen for the proposed system are ISO IEC 9126 standard, which provides guidelines for introducing usability and accessibility in the system[3],[20], Federated Identity Management standard and Windows Identity Framework, which is included to ensure privacy and security to the information of the users[8],[22].

The 32 chosen attributes bear great relevance for the design of the system; therefore, the presence of these attributes can be seen in Figure 2, which highlights where each attribute is applied in the proposed system. The attributes are described in detail in the following three subsections.

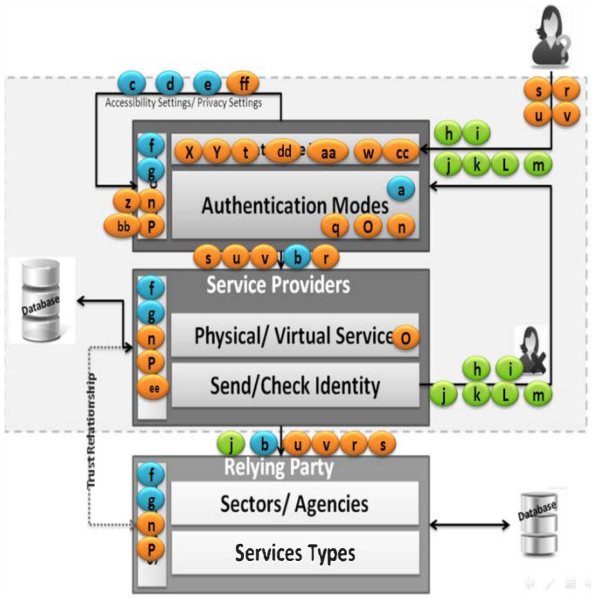

Figure 2. Presence of 32 attributes in UbIAMS

1) Security and Identity Attributes

*Two-factor authentication (a):*multiple authentication modes have been shortlisted for the proposed system; therefore, the attribute of 'two-factor authentication' is present.

Nonce-based authentication (b): the communication between the components of 'Relying Party' and 'Service Providers' is nonce-based, rather than time stamped. The same mechanism has been adopted for communication between the front end layer of the application and service providers and the UbIAMS database and the service provider layer.

User anonymity (c): effective privacy settings have been offered to users so that they can protect their identity and remain anonymous in their communications with other parties.

Control of information (d): privacy settings also give users the freedom to control the flow of their information so that they can inhibit the transfer of information to undesired sources.

Conceal information (e): privacy settings enable the user to conceal or reveal any type of information that they might consider vulnerable or sensitive.

Security Certificates (f): the proposed system is equipped with security certificates facilitating compliance with the security standards implemented in the model.

WS Federation Specification (g): the proposed system is equipped with WS federation specification facilitating compliance with security standards implemented in the system.

2) Accessibility and Acceptability Attributes

As stated previously, the second-chosen criterion for the system is accessibility and acceptability. The attributes of this criterion are present in the following places in the system;

Incremental Learning (h): the interface layer of the model has been designed in such a manner that it facilitates incremental learning for the user according to the chosen standards. Complex operations are split into simpler functions to ensure that the user is able to use the system with ease. The user might not be able to present his identification in the correct manner; therefore, the attribute of incremental learning is present in the system to teach the user the most appropriate way of presenting the identification document or biometrics.

Linearity (i): the interface layer provides functions and operations in an organised sequence for effective learning. Any single process can be learnt through means of similar and simpler steps as opposed to causing confusion through amalgamating different functions. Upon the unsuccessful identification of the user, the user explained the method of successful log-in through easier steps and functions.

Scaffolding (j): the interface layer is developed so as to guide the user in terms of what skills might be needed to make the operations of the system easier. In case the user is not able to log-in successfully, the system will advise of the factors that might have gone wrong in the log-in attempt to inform the user about what needs to be learnt and rectified in the process. The attribute of scaffolding is also present in the communication between the relying parties and service providers since the relying parties may provide some information concerning the authentication process that is required for users to learn in order to access the service.

Learning control (k): the interface layer is designed to cater to the learning pace of all types of users; therefore, the user can choose to alter the speed of learning if needed. Unsuccessful login screens also facilitate the provision of learning control to the user.

Accommodating to the learner's style (l): the interface layer has been designed to offer various learning styles as there may be different types of user (with varying needs and capabilities). The unsuccessful log-in process and interface is also designed to cater to differing user learning styles.

Intermittent feedback (m): feedback is important for systems to continue evolving and improving. The interface layer asks the user relevant questions to inquire about the level of acceptability of their experience and the factors that can be addressed to improve the operations. Intermittent feedback is also aimed to be gained from the unsuccessful login screens.

3) Usability and User Experience Attributes

Following extensive research, the third criterion of attributes chosen is usability and user experience. The proposed system has been made compliant with the following attributes:

User diversity (n): in the presence of such differences of capabilities and needs, just one specific system would not have been suitable; therefore, a generic system needs to be designed. User diversity has been introduced in the system with the aid of the standards chosen. User diversity has also been catered for in the authentication modes so that the user can choose the preferred mode according to convenience.

Controllability (o): controllability has been introduced in the proposed system in the authentication modes so that the user can present proof of identity in an effective manner. It is also present in the interoperability aspect of the model between the two spaces (physical and virtual) to ensure that the user reaches the destination of his choice.

Aesthetics (p): aesthetics have been introduced in the system as per the standards chosen for the model.

Technology variety (q): due to the abundance of technologies and environments, the proposed system has been made compatible with a wide range of technologies to facilitate smooth functioning. Compliance with a variety of technologies has been offered in authentication modes.

Attitude (r): the attitude maintained in the model is helpful and encouraging. The welcome notes and initial steps of the system possess a facilitating tone to encourage the user to utilise the service and make it easy for him. Communication between the three layers also has a facilitating tone to ensure continued cooperation between the participating parties.

Consistency (s): there exists consistency of information and functions which are exposed to the user through the interface of the system; this makes operations easier to grasp and comprehend. There also exists consistency in the system of communication between the different layers and participating units of the system so that there is no discrepancy.

Multiple language support (t): the interface layer of UbIAMS is equipped with multiple language support to make the system operable through a wide range of users rather than a selected segment of users belonging to a certain region.

Effectiveness (u): it is ensured that the user is able to perform system operations effectively. Extensive measures have been taken to ensure that the attribute of effectiveness is present in the communication between the participating units' first layer (interface layer) and second layer (identification and interoperability layer), and the second layer and relying parties' layer.

Efficiency (v): the communications between the layers are also equipped with such a mechanism that ensures the performance of operations in the least possible times. Efficiency is also witnessed in the system in the form of the pace of operations and the functions offered to the user.

Helpfulness (w): the interface layer is designed in such a manner that the user can find help regarding the performance of all functions. Such help facilitates effective utilisation of the functions and features of the system.

Learnability (x): the interface layer has been designed to facilitate effective and fast learning for all types of users.

Memorability (y): the interface layer offers functions and operations in such a logical manner that they can be easily memorised by the user.

Robustness (z): as per the chosen standards, the features and operations of the proposed system are robust in nature.

Simplicity (aa): the interface layer offers the functions and operations in such a simple and easy manner that users will not take much time in grasping the mechanism of the system.

Self-descriptiveness (bb): the interface layer offers self-descriptiveness in all of its functions; these self-descriptive factors are incorporated within the system according to the standards chosen.

Perceived Affordance (cc): the functions on the interface layer are shaped such that their perceived actions can be understood by the users.

Mapping (dd): the functions are located on the interface layer such that their context relates to the purpose and logic of the operations.

Constraints (ee): the layer intended for identification and interoperability implements the attribute of constraints according to the chosen standards.

Convention (ff): as stated earlier, accessibility and privacy settings are provided by the interface layer of the system, which offer customisations to which the users are accustomed.

B. Comparing with Similar Systems

Some of existing systems have been analysed and shown in TABLE II, which summarises a critical review of an extensive evaluation of existing systems with the identified 32 attributes. A tick (✔) means that there is strong evidences showing the system of such criteria according to specific references; however, a cross(✘) means there is no any evidence to suggest that. Finally, a questionmark (?) means that there is no information concerning such criteria.

TABLE II. COMPARISON OF DIFFERENT SYSTEMS

	ENCF	STORK	GIF	FEGIMA	UAENC
a	✔[26-8]	✔[27]	✘[10]	?	✔[3]
b	?	✘[11]	?	?	?
c	✔[9]	?	✔[29]	✔[18-19]	✘[12]
d	✔[16]	✔[24]	✔[26]	✔[18-19]	✘[12]
e	✔[16]	✔[24]	✔[26]	✔[18]	✘[12]
f	✔[2-26]	✔[27]	✔[10-28]	✔[18]	✔[3]
g	✘[2-9]	✘[27]	✘[10]	✘[18]	✘[3]
h	?	?	✘[10]	?	✔[12]
i	?	?	✘[10]	?	?
j	?	?	✘[10]	?	✔[12]
k	?	?	✘[10]	?	?
l	?	?	✔[10]	?	?
m	?	?	?	?	?
n	?	✔[11]	✔[10-29]	?	?
o	?	?	?	?	✔[3]
p	?	?	✔[10]	?	✔[3]
q	✔[2-9]	✔[24]	✔[10]	✔[18]	✔[3]
r	?	✔[11]	?	?	✔[3]
s	?	?	?	?	✔[3]
t	?	✔[24]	✔[10]	?	?
u	✔[16]	✔[27]	✔[10]	?	✔[3-12]
v	✔[16]	✔[27-11]	✔[10]	?	✔[3-12]
w	✘[16]	✔[11]	✔[10]	?	✔[3]
x	✘[16]	✔[11]	✔[10]	?	✔[3]
y	✔[16]	✔[11]	✔[10]	?	✔[3]
z	✔[2-26-8]	✔[27]	?	?	✔[3]
aa	✘[16]	✔[11]	✔[10-29]	?	✔[3]
bb	✘[16]	✔[11]	✔[10]	?	✔[3]
cc	✘[16]	✔[11]	?	?	✔[3]
dd	✘[16]	✔[11]	✔[26]	?	✔[3]
ee	✔[9]	?	✔[10]	?	?
ff	?	?	✔[10]	?	?

A more detailed critical review and evaluation of existing systems will be presented in the conference.

IV. CONCLUSION AND FUTURE WORK

The extensive study of the existing frameworks and relevant theories enabled understanding of the requirements of integration of physical and virtual identity management systems from the three perspectives: Security, Acceptability and User Experience. However, there is no research known that considers the integration of physical and virtual identity management systems from the user's viewpoint; therefore, this paper proposed the UbIMAS System that would conform to the standards of these three perspectives for different users and sectors. User and expert evaluations are being conducted to validate the components of UbIAMS. Such evaluation activities will be discussed in detail in future papers.

REFERENCES

[1] C. Steinfield, "Combining Physical and Virtual Channels: Opportunities, Imperatives and Challenges", *14th Bled Electronic Commerce Conference*, June 25 - 26, 2001. www.msu.edu/~steinfie/Bledfinal.pdf *(Access Date: 20 May, 2012)*

[2] P. N. Chhanabhai, "First impression of operating system styles affect usability", University of Otago, 2004. http://otago.ourarchive.ac.nz/handle/10523/1205 *(Access Date: 20 May, 2012)*

[3] A. M. Al-Khouri, "UAE National ID Programme Case Study", *International Journal of Human and Social Sciences*, Vol. 1, No. 2, 2006. www.waset.org/journals/ijhss/v1/v1-2-11.pdf *(Access Date: 20 May, 2012)*

[4] L. M. Chan, M. L. Zeng, Metadata Interoperability and Standardization – A Study of Methodology Part I, *D-Lib Magazine,* Volume 12, Number 6, 2006. http://www.dlib.org/dlib/june06/zeng/06zeng.html *(Access Date: 20 May, 2012)*

[5] R. L. Morgan, S. Cantor, S. Carmody, W. Hoehn, K. Klingenstein, "Federated Security: The Shibboleth Approach", *Educause Quarterly*, Number 4, 2004. http://www.educause.edu/EDUCAUSE+Quarterly/EDUCAUSEQuarterlyMagazineVolum/FederatedSecurityTheShibboleth/157315 *(Access Date: 20 May, 2012)*

[6] M. O. Leavitt, B. Schneiderman, "Chapter 3: Accessibility" in *Research-Based Web Design & Usability Guidelines*, ISBN 0-16-076270-7. www.usability.gov/pdfs/chapter3.pdf *(Access Date: 20 May, 2012)*

[7] Nielsen Norman Group Report, *Email Newsletter Usability 4th Edition*, 2006.

[8] A. Poller, U. Waldmann, S. Vowe and S. Turpe, "Electronic Identity Cards for User Authentication- Promise and Practice", *IEEE*, 2010. http://www.computer.org/portal/web/csdl/doi/10.1109/MSP.2011.148 *(Access Date: 20 May, 2012)*

[9] S. Arora, "National e-ID card schemes: A European overview", *Information Security Technical Report*, Vol. 13, pp 46-53, 2008. http://www.sciencedirect.com/science/article/pii/S1363412708000241*(Access Date: 20 May, 2012)*

[10] H. Graux, G. Lambert, B. Jossin, E. Meyvis, "Study on Mutual Recognition of eSignatures: update of Country Profiles", *IDABC Programme*, 2009. http://ec.europa.eu/idabc/servlets/Doca7bf.pdf?id=32436 *(Access Date: 20 May, 2012)*

[11] D. Berbecaru, E. Jorquera, M. Schiavo, A. Johnston, A. Lioy, A. F. Axfjörð, C. Luyten, "D5.7.2 Functional Design for PEPS, MW models and interoperability", *STORK-eID Consortium*, 2010. https://www.eid-stork.eu/ *(Access Date: 20 May, 2012)*

[12] A. M. Khouri, "Targeting Results: Lessons Learned from UAE National ID Program", *Proceedings of the 2011 International Conference on Industrial Engineering and Operations Management Kuala Lumpur,* 2011. www.eida.gov.ae/userfiles/GJCAT_2012_0104.pdf *(Access Date: 20 May, 2012)*

[13] B. Shneiderman, "Universal Usability", *Communications of the ACM*, Vol. 43, No. 5, 2000. http://dl.acm.org/citation.cfm?id=332843 *(Access Date: 20 May, 2012)*

[14] I. Ajzen, "The theory of planned behavior". *Organizational Behavior and Human Decision Processes*, Vol. 50, No. 2, pp. 179-211, 1991. http://www.cas.hse.ru/data/816/479/1225/Oct%2019%20Cited%20%231%20Manage%20THE%20THEORY%20OF%20PLANNED%20BEHAVIOR.pdf *(Access Date: 20 May, 2012)*

[15] A. Yusoff, R. Crowder, L. Gilbert and G. Wills, "A Conceptual Framework for Serious Games", *Ninth IEEE International Conference on Advanced Learning Technologies*, 2009. *http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5194153&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5194153 (Access Date: 20 May, 2012)*

[16] S. Arora, "Review and Analysis of Current and Future European e-ID Card Schemes", University of London, 2007. http://www.ma.rhul.ac.uk/static/techrep/2008/RHUL-MA-2008-07.pdf *(Access Date: 20 May, 2012)*

[17] A. Overeem and J. Oosten, "Towards a Pan European e-ID Interoperability Infrastructure", *Proceedings of the 42nd Hawaii International Conference on System Sciences,* 2009. *http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4755352&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4755352 (Access Date: 20 May, 2012)*

[18] M. Naderi, J. Siddiqi, B. Akhgar, W. Orth, N. Meyer, M. Tuisku and G. Pipan, "Towards a Framework for Federated Global Identity Management", *International Journal of Network Security,* Vol.7, No.1, pp.88-99, 2008.http://ijns.femto.com.tw/contents/ijns-v7-n1/ijns-2008-v7-n1-p88-99.pdf *(Access Date: 20 May, 2012)*

[19] J. Siddiqi, B. Akhgar, M. Naderi, S. Hallam, W. Orth, N. Meyer, M. Tuisku, G. Pipan, "Federated Global Identity Management: Towards a Framework", *2006 International Conference on Grid Computing & Applications* 2006.http://citeseerx.ist.psu.edu/messages/downloadsexceeded.html*(Access Date: 20 May, 2012)*

[20] National Institute of Standards and Technology, "ISO/IEC 24727 General Concepts & Terminology", *ISO/IEC Workshop December*, 2009. http://csrc.nist.gov/news_events/ISO_IEC-24727Tutorial/presentations/day1/day1_1230_iso24727-general-concepts-and-terminology.pdf *(Access Date: 20 May, 2012)*

[21] Y. P. Liao, S. S. Wang, "A secure dynamic ID based remote user authentication scheme for multi-server environment", *Computer Standards & Interfaces*, Vol. 31, pp 24–29, 2009. http://personnel.sju.edu.tw/%E6%94%B9%E5%96%84%E5%B8%AB%E8%B3%87%E7%A0%94%E7%A9%B6%E6%88%90%E6%9E%9C/98%E5%B9%B4%E5%BA%A6/%E8%91%97%E4%BD%9C/43.pdf *(Access Date: 20 May, 2012)*

[22] L. Beslay, Y. Punie, "The Virtual Residence: Identity, Privacy and Security", Publisher: European Commission, Institute for Prospective Technological Studies (IPTS), Joint Research Center, Vol. 67.

[23] A. Karantjias, T. Stamati, N. Polemi, D. Martakos, "A synchronous, open, user-centric, federated Identity and Access Management System (OpenIdAM)", *Electronic Journal of Emerging Tools and Applications,* Vol 3,Issue 1. http://www.ejeta.org/specialOct09-issue/ejeta-special-09oct-4.pdf *(Access Date: 20 May, 2012)*

[24] Portal Administración electrónica, "STORK- Secure Identity across Borders Linked. European Union", n.d. http://administracionelectronica.gob.es/recursos/pae_000001611.pdf *(Access Date: 20 May, 2012)*

[25] I. Wechsung, A. B. Naumann, R. Schleicher, "Views on Usability and User Experience: from Theory and Practice", Deutsche Telekom Laboratories, 2008. http://www.cs.uta.fi/~ux-emotion/submissions/Wechsung-etal.pdf *(Access Date: 20 May, 2012)*

[26] S. Ahlswede, "eIDs in Europe", Deutsche Bank Research, 2010. http://www.finextra.com/Finextra-downloads/featuredocs/PROD0000000000262236.pdf *(Access Date: 20 May, 2012)*

[27] V. A. Navarro, J. Gumbau, P. Santapau and A. Marzal, "STORK project results: Pan-European eID interoperability demonstrated", 2011. http://www.eunis.ie/abstracts/STORK-Project-Results_PaulSantapau_Abstract.pdf *(Access Date: 20 May, 2012)*

[28] M. Faher, "eEpoch- (eEurope Smart Card Charter proof of concept and holistic solution)", *2nd eEpoch Open Conference*, 2003. *http://www.eepoch.net/documents/public/deliverables/eEpoch_D33.pdf (Access Date: 20 May, 2012)*

[29] B. Rouchouze, "European eServices: What is missing for interoperability?", Gemalto, 2009. *http://www.eurim.org.uk/activities/ig/idg/Gemalto-What_is_missing_for_Interoperability.pdf (Access Date: 20 May, 2012)*

[30] D. Garlan and B. Schmerl, "Using Architectural Models at Runtime: Research Challenges", *Proceedings of the European Workshop on Software Architectures, St. Andrews, Scotland,* May 2004. *http://www.springerlink.com/content/w68h7xb07x67duwf/ (Access Date: 20 May, 2012)*