# IAMS Framework: A New Framework for Acceptable User Experiences for Integrating Physical and Virtual Identity Access Management Systems

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

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

*Abstract*— **The modern world is populated with so many virtual and physical Identity Access Management Systems (IAMSs) that individuals are required to maintain numerous passwords and login credentials. The tedious task of remembering multiple login credentials can be minimised through the utilisation of an innovative approach of single sign-in mechanisms. During recent times, several systems have been developed to provide physical and virtual identity management systems; however, most have not been very successful. Many of the available systems do not provide the feature of virtual access on mobile devices via the internet; this proves to be a limiting factor in the usage of the systems. Physical spaces, such as offices and government entities, are also favourable places for the deployment of interoperable physical and virtual identity management systems, although this area has only been explored to a minimal level. Alongside increasing the level of awareness for the need to deploy interoperable physical and virtual identity management systems, this paper addresses the immediate need to establish clear standards and guidelines for successful integration of the two mediums.**

***Keywords- IAMS Framework; Acceptable User Experiences; Physical and Virtual Identity Access Management Systems***

## I. Introduction

An extensive literature review has been conducted to study the existing systems that address identity management in physical and virtual spaces. The study has revealed that many countries, such as those within Europe [4] and the Middle East [5] etc. have taken the initiatives of providing their citizens with convenience and greater security measures with the introduction of different identity tokens (such as smart cards, biometrics, PINs, passwords, etc.) in physical and virtual spaces identity management. Gemalto published a research paper highlighting the efforts of the Belgian government to introduce smart cards and PIN as the authentication mechanism of individuals in both physical and virtual spaces [38-23]. Their systems provide access to only a few specific government agencies and internet services. The Austrian government has implemented the concept of integrated authentication systems in a most innovative way; the mandatory presence of a specific identity token has been eliminated from their systems [2]. Any mobile device or smart card—such as health insurance card or bank card, for example—can be used to serve as a Citizen Card that can provide access; however, the integration of the physical and virtual spaces is not mentioned in their systems. Al-Khouri discusses the endeavours that have been witnessed in UAE; the authentication mechanism has been incorporated with digital certificates of Public Key Infrastructure (PKI) capabilities [3]. The individuals are identified on the basis of their finger prints and palm prints. The identity management systems have been deployed for very few government gencies and the online spaces of the users. Dray provides examples of systems that provide interoperability between physical and web spaces; they can be used as e-passports and also provide entry to ships and ports [2],[3],[4],[5]. After conducting a thorough study of the available interoperable authentication systems, it has been established that the success rate of the interoperability between physical and virtual spaces has not been encouraging. In addition, no system has been found through research activities that would successfully address the specific needs of the customers to make experience acceptable and accessible. Moreover, a few features and functions should also be introduced that can make the whole experience more accessible and secure. With this in mind, this paper shall focus mainly on acceptability, which includes accessibility; user experience involving usability; and security, containing identity since the existing systems are most lacking in addressing these aspects.

The paper is structured in the following manner: firstly, a background of the relevant theories and suitable attributes are explained in *Section 2*, which is followed by a critical review and comparison of existing frameworks with different criteria and selected attributes in *Section 3*; subsequently, *Section 4* proposes IAMS Framework; and finally, *Section 5* concludes with a summary of the paper and the future planned research.

## II. Relevant Theories and Suitable Attributes

### *A. Security and Identity*

The security and identity of user information in the physical and virtual worlds has been an area of interest and concern for many years. A number of theories have been developed in the past with the objective to improve the security and identity. One of the most significant theories for securing authentication protocol for multi-server environment using dynamic ID was written by Liao andWang [1]. Their theory relies on the nonce-

978-1-908320-04/9/$25.00©2012 IEEE

based (a value or counter) mechanism rather than timestamp. The authentication key of the user is based on two factors such that the theft of one cannot be used to recreate the other, thereby improving the level of security. The theft of the past session key cannot serve to provide access to any individual twice since the key is nonce-based and unique every time. User anonymity is protected through the dynamicity of the variables of the login session. Importantly, these authors have not implemented their approach in the physical environments; however, the attributes of their theory seem effective enough in terms of facilitating a secure service on multi-server environments.

It is important to provide an individual with certain rights to control the exposure of his personal information, thus enhancing the level of privacy and security of the data. To address this, the concept of virtual residences was developed by Beslay and Punie, who applied it to identity management systems [7-8]. It promotes the implementation of common concepts of boundaries in the online world—just like they are implemented in the real world. The level of security and control available to the users in the real world is expected to be present in the online world as well. Beslay and Punie have highlighted three main aspects that need to be considered so as to ensure effective interoperable identity management in online and offline spaces, namely ‘Control of personal information’, ‘Clear mapping between physical and virtual identity’, and ‘Conceal information’.

The last selected theory in this section explains the implementation of the concept of e-ID federation, which provides access across multiple platforms since it can serve as the basis of the authentication mechanism for the chosen research study [9]. The e-ID federation implements a security token service (STS) that is based on the Windows Identity Framework. The authentication mechanism is based on security certificates, login forms, Windows Authentication and OpenID credentials [10]. A common platform is established by the STS, which can be accessed by different sources to authenticate the individuals. The interoperability takes place on an intermediate layer that serves as an abstraction of the authentication mechanism.

### B. *Acceptability and Accessibility*

Acceptability is the new term for adequacy in regard to satisfying a need, requirement or standard, i.e. satisfactory for the user's needs, which involves accessibility needs [36]. There are various imperative theories that study users' acceptability and predicts the level of user intentions to use the system; the Technology Acceptance Model (TAM) is one of them. TAM has been influenced by an earlier theory of Azjen and Fishbein’s Theory of Reasoned Action (TRA) [11]. Behavioural intention is defined as the attitude of the individual and the way in which the individual is expected to act in relation to the people around him. The performance of any person is judged by his behavioural intentions. TAM is based on two variables that denote the level of acceptance for the service or application: usefulness and ease of use. Similar attributes can prove to be useful for devising a framework for interoperable identity management system for physical and virtual spaces. Moreover, the attributes based on learning and pedagogy theory can also be helpful for the research study [14]. Pedagogy theory revolves around the actions that impart knowledge [13]. The authors have formed a conceptual model based on pedagogy theory, learning, and gaming requirements [13-14]. This conceptual model has been selected as the model is directed towards the identification of attributes that make the user’s experience both acceptable and accessible.

### 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 a lot of organisations that have proposed usability theories and their associated components. One of the most imperative theories addresses the needs of the experienced users, as well as a broader set of users and technologies by introducing universal usability in internet-based and other services [15].Moreover, Perlman's theory partitions the usability aspects into different structures, namely function, platform and language [16]. However, Jakob Nielsen explains that user experience is greatly based on emotions rather than efficiency [6]. Usability focuses on developing and designing better products, whereas user experience focuses on making people happier. Both of these concepts are considered to be different, although they overlap. It also includes the attributes of Jakob Nielsen’s usability theory, which is based on cognitive science and is intended for designing information-based websites. [6],[17]. Besides, Donald Norman’s theory and Jessie James Garrett's theory address the needs of experienced users, as well as designing anything to be used by humans, from physical objects to computer programs to conceptual tools [18],[12]. More specifically, it focuses on emotional design and users’ feelings before, during and after using any system [18].

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

TABLE I. CHOSEN ATTRIBUTES FOR THE DESIGN

| | Attributes | Label |
|---|---|---|
| Security | Two factor authentication [1] | A |
| | Nounce-based authentication [1] | B |
| | User Anonymity [1] | C |
| | Control of information [7-8] | D |
| | Conceal Information [7-8] | E |
| | Security Certificates [9-10] | F |
| | WS Federation Specification [9-10] | G |
| Acceptability | Incremental Learning [11-14] | H |
| | Linearity[11-14] | I |
| | Scaffolding [11-14] | J |
| | Learning Control [11-14] | K |
| | Accommodating to the learner’s style [11-14] | L |
| | Intermittent feedback [11-14] | M |

| | | |
|---|---|---|
| User Experiences | User Diversity [15] | N |
| | Controllability [17],[6] | O |
| | Aesthetics [17],[6] | P |
| | Technology Variety [15] | Q |
| | Attitude [17],[6] | R |
| | Consistency [17],[6] | S |
| | Multiple Language Support [16] | T |
| | Effectiveness [17],[6] | U |
| | Efficiency [17],[6] | V |
| | Helpfulness [17],[6] | W |
| | Learnability [17],[6] | X |
| | Memorability [17],[6] | Y |
| | Robustness [17],[6] | Z |
| | Simplicity [17],[6] | AA |
| | Self-descriptiveness [17],[6] | BB |
| | Perceived Affordance [17],[6] | CC |
| | Mapping [17],[6] | DD |
| | Constraints [17],[6] | EE |
| | Convention [17],[6] | FF |

## III. Comparison with Similar Frameworks

The Global e-ID has been an area of interest and concern for many years. Numerous frameworks and applications have been developed in the past with the objective to improve the security, acceptability and user experiences; some of these have been analysed here on the basis of 32 attributes, which are based on the researched theories of the three perspectives. The idea behind isolating these criteria was to enable a robust comparison of the frameworks and applications' features, advantages and disadvantages, which would eventually lead to the development of IAMS Framework.

### *A. Existing Frameworks*

#### *1) European National e-ID card framework (ENCF)*

It finds its origin from the European countries where it is being implemented to integrate the physical spaces with the virtual spaces. Some of the examples of this interoperability include digital signatures with the aid of e-ID, with such signatures bearing legal validity [2], compatibility with the financial institutions, the ability to login in the WLANs, the identification and age verification for adult-oriented activities, such as online gambling [21], handling tax applications and declarations on the web, and government services [21].

#### *2) STORK*

An endeavour aiming to provide a framework for implementing cross-border identity management systems in European countries with interoperability between physical and virtual spaces [23-24]. It aims to integrate 17 European countries in the program and 38 public and private organisations.

#### *3) Global Interoperability Framework (GIF)*

Developed on the basis of Identification, Authentication and Electronic Signature (IAS). Interoperability between different types of smart card schemes is sought to be achieved by means of this framework. The scope of this framework covers the e-government services, as well as the internet services utilised and authenticated through means of smart cards [27].

#### *4) FEderated Global Identity MAnagement framework (FEGIMA)*

. Considered to be an innovative security mechanism since they base their authentication process on a diverse range of technologies. This frees the framework from being constrained to one type of technology and offers interoperability with numerous platforms [31]. However, this framework has not been explored by many researchers as only a few research papers could be found related to this framework.

#### *5) UAE National ID Cards(UAENC)*

An endeavour framework concerned with integrating the e-government agencies with the e-commerce services to increase convenience and security for the citizens of UAE. The centralised mechanism of authenticating citizens aims to reduce instances of identity thefts in the respective region [3].

### *B. Comparing Existing Frameworks*

Many frameworks and applications have been developed in the past with the objective to improve the security, acceptability or user experiences on Global e-ID; however, there lacks a framework that focuses on all these three aspects together. Some of these frameworks have been analysed in TABLE II, which summarises a critical review of an extensive evaluation of existing frameworks with various 32 attributes. A tick (✓) means that there is strong evidences showing the frameworks of such criteria according to specific references; however, a cross (✗) means there is no any evidence to suggest that these frameworks offer the required criteria. Finally, a question mark (?) means that there is no information concerning such criteria.

TABLE II. Comparison of different frameworks

| | ENCF | STORK | GIF | FEGIMA | UAENC |
|---|---|---|---|---|---|
| a | ✓ [20-21] | ✓ [24] | ✗[27] | ? | ✓[3] |
| b | ? | ✗ [38-26] | ? | ? | ? |
| c | ✓[19] | ? | ✓[29] | ✓[31-32-33] | ✗[34] |
| d | ✓[21] | ✓[25] | ✓[30] | ✓[31-32] | ✗[34] |
| e | ✓[21] | ✓[25] | ✓[30] | ✓[31] | ✗[34] |
| f | ✓ [2-20] | ✓[24] | ✓[27-28] | ✓[31] | ✓[3] |
| g | ✗ [2-19] | ✗[24] | ✗[27] | ✗[31] | ✗[3] |
| h | ? | ? | ✗[27] | ? | ✓[34] |
| i | ? | ? | ✗[27] | ? | ? |
| j | ? | ? | ✗[27] | ? | ✓[34] |
| k | ? | ? | ✗[27] | ? | ? |
| l | ? | ? | ✓[27] | ? | ? |
| m | ? | ? | ? | ? | ? |
| n | ? | ✓[26] | ✓ [27-29] | ? | ? |
| o | ? | ? | ? | ? | ✓[3] |

| | | | | | |
|---|---|---|---|---|---|
| p | ? | ? | ✓[27] | ? | ✓[3] |
| q | ✓[2-19] | ✓[25] | ✓[27] | ✓[31] | ✓[3] |
| r | ? | ✓[26] | ? | ? | ✓[3] |
| s | ? | ? | ? | ? | ✓[3] |
| t | ? | ✓[25] | ✓[27] | ? | ? |
| u | ✓[21] | ✓[23] | ✓[27] | ? | ✓[3-34] |
| v | ✓[21] | ✓[23-26] | ✓[27] | ? | ✓[3-34] |
| w | ✗[22] | ✓[26] | ✓[27] | ? | ✓[3] |
| x | ✗[22] | ✓[26] | ✓[27] | ? | ✓[3] |
| y | ✓[21] | ✓[26] | ✓[27] | ? | ✓[3] |
| z | ✓[2-20-21] | ✓[23] | ? | ? | ✓[3] |
| aa | ✗[22] | ✓[26] | ✓[27-29] | ? | ✓[3] |
| bb | ✗[22] | ✓[26] | ✓[27] | ? | ✓[3] |
| cc | ✗[22] | ✓[26] | ? | ? | ✓[3] |
| dd | ✗[22] | ✓[26] | ✓[30] | ? | ✓[3] |
| ee | ✓[19] | ? | ✓[27] | ? | ? |
| ff | ? | ? | ✓[27] | ? | ? |

A more detailed critical and extensive review and evaluation of existing frameworks with these attributes will be presented in the conference. Following the analysis of the existing frameworks, the need for an efficient framework for integrating physical and virtual identity access management systems has been presented in the next section.

## IV. Proposed IAMS Framework

The framework will facilitate the structuring of the attributes that are based on the researched theories of the three perspectives. The following steps will be followed to develop the IAMS framework:

### A. *Group Attributes with Similar Themes*

New themes have been added to categorise the attributes and to incorporate them within the framework. The themes have been allocated on the basis of the following factors:

#### 1) *Authentication Mechanism (a-b)*

The authentication mechanism has much relevance in any access management system. Two-factor authentication and nonce-based authentication both play a role in the reliable authentication of the user; therefore, they can be grouped under a single theme.

#### 2) *Privacy (c-d-e)*

Privacy involves the aspects of anonymity, secrecy and autonomy [35], which reflect the true definition of privacy. Accordingly, these can be grouped together under a single theme.

#### 3) *Security standards (f-g)*

A system tends to offer a greater level of security and offers greater reliability if effective security standards are followed within the development phases. Such an approach has been used in the development of the IAMS framework since security certificates and WS federation specification have been chosen as its security standards.

#### 4) *Ease of Learning (h-i)*

The process of learning can be made easier if incremental learning is present, i.e. if the complex tasks are broken into smaller and simpler tasks. However, incremental learning would not be effective if it is not coupled with the logical flow of functions and linearity. The combination of such attributes makes the learning process easier; therefore, these can be grouped under a single theme of 'ease of learning'.

#### 5) *Facilitation for Learning (j-k-l-m)*

These attributes provide the user with different modes through which the learning process can be improved and facilitated: for example, scaffolding notifies the factors that should be learned to improve functioning of the system. Learning control facilitates the user to maintain his desired pace at performing and learning the functions. Accommodating to the learner's style will help the user to overcome the limitations commonly witnessed in system operations since they are designed for a specific set of users. Intermittent feedback will facilitate the constant improvement of the system, thus making the learning process easier for users.

#### 6) *Cultural Aspects (n-o-p-q-ff)*

Cultural aspects have been found to exist at minimal levels in the prevailing systems, and so the consideration for different types of users (people with disabilities, non-technically experienced, etc.), compliant technologies, representation of the screens and objects and other traditional factors of different cultures play an important role in the system. The provision of such attributes within the system promotes controllability since the user will be more confident and comfortable with the cultural settings of his choice.

#### 7) *Nature of Content (r-s)*

The content of a system bears great relevance since commendable functions will not prove to be effective for the users if the content is not placed in a logical flow. Another important aspect of content is the tone of the content (attitude) that encourages the user to avail the system for different services.

#### 8) *Performance Measure(u-v-z)*

The presence of performance measures is vital for the evaluation of any system and service. The most common forms of performance measures include effectiveness, efficiency and robustness.

#### 9) *Ease of Interaction (t-w-x-y)*

The effectiveness of functions of any systems depends on the level of interactivity and convenience offered by them. Multiple language support enables the user to interact with the system with ease since he is able to understand all the available functions and services in his own language. The attribute of 'helpfulness' provides aid to the user to interact with the system in the most convenient manner. The learnability and memorability of functions and services in the system enable the user to interact with the system at a faster pace; such attributes facilitate ease of interaction with the system, and can therefore be grouped under the single theme of 'ease of interaction'.

*10) Relational Factors (aa-bb-cc-dd-ee)*

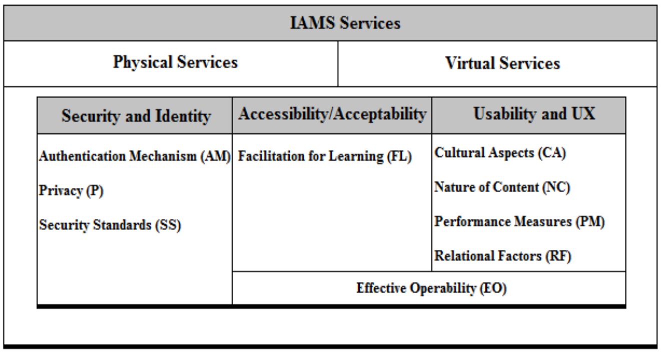
The functions of the system should be offered in accordance with their descriptions (self-descriptiveness), perceived actions (perceived affordance), context of their location (mappings) and limitations that might be associated with a specific function (constraints). It is aimed to keep the relations simple to ensure that the user does not feel disoriented in the presence of numerous functions.

### *B. Reclassify Components*

After analysing the classification of themes and components, it can be seen that there exists some degree of overlap between them. For example, ease of interaction and ease of learning both facilitate smooth operation of functions in the system. It can also be stated that incremental learning tends to increase learnability and memorability of the functions and vice versa. Therefore, it would not be wrong to amalgamate the two themes of 'Ease of interaction' and 'Ease of Learning' into a single theme of 'Effective operability'. In other words, it can be stated that operability of the system can be made more effective if the system is equipped with incremental learning, linearity, multiple language support, helpfulness, learnability, and memorability. Therefore, the process of reclassification creates the 9 themes for 32 attributes.

### *C. Constructing the Framework*

The IAMS framework is developed with the aim of allowing the conceptualisation and development of user-centred system that facilitates the presence of a secure environment. The user-centred system shall also facilitate accessibility and usability for all kinds of users.



IAMS Services

Physical Services

Virtual Services

Security and Identity

Authentication Mechanism (AM)

Privacy (P)

Security Standards (SS)

Accessibility/Acceptability

Facilitation for Learning (FL)

Usability and UX

Cultural Aspects (CA)

Nature of Content (NC)

Performance Measures (PM)

Relational Factors (RF)

Effective Operability (EO)

Figure 1. Structure of the IAMS framework

It can be seen from Figure 1 that the three perspectives are given at the top of each proposed themes—namely security and identity, accessibility and acceptability, and user experience and usability. The main component of the framework constitutes the services offered to the users in the physical as well as virtual worlds. The other component in the framework includes the themes for chosen attributes that have been categorised with respect to the three perspectives under consideration.

- Security and identity has the following themes: authentication mechanism (AM), privacy (P) and security standards (SS).
- Acceptability and accessibility has a theme of facilitation of learning (FL).
- User experience and usability has the following themes: cultural aspects (CA), nature of content (NC), performance measures (PM), relational factors (RF).
- Effective operability (EO) is being shared amongst the accessibility and usability perspectives.

## V. 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 different perspectives—security, acceptability and user experience. However, there is no research currently known that considers the integration of physical and virtual identity management systems from the users' viewpoint. Therefore, this paper describes the integration of physical and virtual identity management systems, based on the proposed IAMS Framework which would conform to the standards of acceptability and accessibility for different users and sectors. An expert evaluation has been designed to measure experts' agreement patterns concerning the components of the IAMS Frameworks. Experts ascertain whether there are some attributes missed and rate the level of the importance and conflict associated with each attribute towards these three dimensions. The expert evaluation's steps as well as the results will be presented in detail in the conference.

## References

[1] Y. P. Liao, S. S. Wang, "A secure dynamic ID based remote user authentication scheme for multi-server environment", *Computer Standards and 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)*

[2] T. Rossler, "Giving an interoperable e-ID solution: Using foreign e-IDs in Austrian e-Government", *Computer law and security report*, Vol. 24, pp 447-453, 2008. http://www.sciencedirect.com/science/article/pii/S0267364908001039 *(Access Date: 21 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] B. P. Bruegger, D. Hühnlein, M. Kreutzer, "Towards global eID-Interoperability", *Biometrics and Electronic Signatures - BIOSIG*, pp. 127-140, 2007. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.88.9615 *(Access Date: 21 May, 2012)*

[5] Laser Card Inc., "The Kingdom of Saudi Arabia National ID Card", 2009. http://www.hidglobal.com/main/documents/casestudy-gov-id-ksa-cs-en.pdf *(Access Date: 21 May, 2012)*

[6] J. Nielsen, "Jakob Nielsen's website", http://useit.com *(Access Date: 21 May, 2012)*

[7] M. Hansen, P. Berlich, "Identity Management Systems: Gateway and Guardian for Virtual Residences", *EMTEL*, 2003. http://citeseerx.ist.psu.edu/messages/downloadsexceeded.html *(Access Date: 21 May, 2012)*

[8] 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.

[9] H. Tsavdaris, "e-ID Federation: Security Token Service implementation using Windows Identity Framework", *Greek Interoperability Center*. http://www.iocenter.eu/demos/e-id-federation-security-token-service-

implementation-using-windows-identity-framework.aspx *(Access Date: 21 May, 2012)*

[10] 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)*

[11] 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)*

[12] J. J. Garrett, *The Elements of User Experience: User-Centered Design for the Web and Beyond*, Peachpit Press , Second Edition , 2002.

[13] I. Webb, "Pedagogy", University of Tasmania, n.d. http://www.educ.utas.edu.au/users/ilwebb/Research/pedagogy.htm *(Access Date: 20 May, 2012)*

[14] 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)*

[15] 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)*

[16] G. Perlman, "Achieving Universal Usability by Designing for Change", *IEEE Internet Computing*, 2002. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=991443&contentType=Journals+%26+Magazines *(Access Date: 20 May, 2012)*

[17] 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)*

[18] D. Norman, "The Design of Everyday Things", *Basic Books*, 2002.

[19] 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)*

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

[21] 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)*

[22] 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)*

[23] 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)*

[24] 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)*

[25] 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)*

[26] 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)*

[27] M. Lange, T. Sprundel, L. Hollander, "Contextual and Conceptual Modelling", *e*-Europe Smart Card Charter, 2002. www.eepoch.net/documents/public/Bibliography/03-1%20GIF%20Part%201_V201.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] National Institute of Standards and Technology, "ISO/IEC 24727 General Concepts and Terminology", *ISO/IEC Workshop December*, 2009. http://csrc.nist.gov/news_events/ISO_IEC-24727 Tutorial/presentations/day1/day1_1230_iso24727-general-concepts-and-terminology.pdf *(Access Date: 20 May, 2012)*

[31] 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)*

[32] 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 and Applications (GCA'06),* 2006. http://citeseerx.ist.psu.edu/messages/downloadsexceeded.html*(Access Date: 20 May, 2012)*

[33] M. Gindonis, "Finnish Grid Activities and M-grid", Helsinki Institute of Physics, 2004. http://www.kbfi.ee/~andi/NordicGrid/uploads/Meetings/2004-10-Link%F6ping-Michael_Kustaa_Gindonis.pdf *(Access Date: 20 May, 2012)*

[34] 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)*

[35] K. A. Taipale, "Data Mining and Domestic Security: Connecting the dots to make sense of data", *Columbia Science and Technology Law Review,* Volume 5, 2003. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=546782 *(Access Date: 20 May, 2012)*

[36] M. Maguire, N. Bevan, "User requirements analysis: A review of supporting methods". *The IFIP 17th World Computer Congress.* Kluwer Academic Publishers. Montreal, Canada, 2002, p133-148. http://dl.acm.org/citation.cfm?id=709394 *(Access Date: 20 May, 2012).*