Validating the IAMS Framework

Sara Jeza Alotaibi, Mike Wald
Electronics and Computer Science, University of Southampton, United Kingdom

Abstract

The wide spread of services on the internet has aggravated the issue of maintaining multiple identities such as the virtual identities that are based on specific login credentials like username, passwords and PINs. On the other hand, multiple physical identities also prove to be difficult to maintain since different sources require the presence of different smart cards, mobile devices or other proofs of identities. This paper addresses the problem of how to design an optimum user experience for Integrating Physical and Virtual Identity Access Management System (IAMS) by combining theories in three research perspectives: Security, which includes identity; User Experience, comprising Usability; and Acceptability, containing Accessibility. Existing research in this area tend to focus on one of these research perspectives. However, there is little evidence that researchers have approached the issue of an overlap and conflict between these three research perspectives with the intent of building a cohesive understanding of Integrating Physical and Virtual IAMSs in e-government domain and the relationships that exist between the different dimensions and components. Consequently, this research has developed a conceptual IAMS Framework for Integrating Physical and Virtual IAMS, and used expert evaluations for validating the components of the framework.

1. 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 [19]. 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 agencies 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; *Section 5* presents the analysis for the experts' evaluation towards the components of the IAMS framework. Finally, *Section 6* concludes with a summary of the paper.

2. Relevant Theories and Suitable Attributes

2.1. 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-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.

2.2. 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 [25]. 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.

2.3. 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], [27]. 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 1 shows the 32 attributes that have been chosen for designing the framework of interoperable identity management systems for physical and virtual spaces:

Table 1. 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**

3. 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.

3.1. Existing Frameworks

3.1.1. 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].

3.1.2. 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 [19-20]. It aims to integrate 17 European countries in the program and 38 public and private organisations.

3.1.3. 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 [22].

3.1.4. 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 [23]. However, this framework has not been explored by many researchers as only a few research papers could be found related to this framework.

3.1.5. 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].

3.2. 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 the above frameworks have been analysed in the previous papers [12], [26], which summarises a

critical review of an extensive evaluation of existing frameworks with various 32 attributes.

4. 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:

4.1. 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:

4.1.1. 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.

4.1.2. Privacy (c-d-e). Privacy involves the aspects of anonymity, secrecy and autonomy [24], which reflect the true definition of privacy. Accordingly, these can be grouped together under a single theme.

4.1.3. 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.

4.1.4. 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'.

4.1.5. 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.

4.1.6. 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.

4.1.7. 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.

4.1.8. 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.

4.1.9. 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'.

4.1.10. 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.

4.2. 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.

4.3. 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.

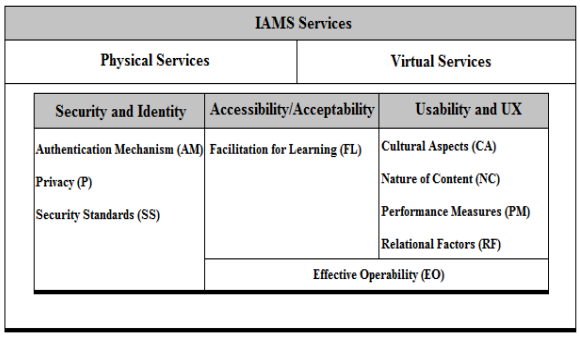

Figure 1. Structure of the IAMS framework

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.

5. Validating the IAMS Framework

Validity considers how well the items of an instrument represent a concept or domain of content [28]. Validation becomes an important step, especially when a new measure is being developed where there is no existing measure that operationalises the concept as the researcher intended [28]. For example, there are instruments measuring security, accessibility, and usability in any system; however, a framework that defines all of these together in terms of identity access management systems or an instrument that measures acceptability and user experience in the context of identity access management systems is new, and thus needs to be validated.

Using a panel of experts during the course of a validation will provide useful feedback concerning the quality of a newly developed measure. Without conducting a validation study, a researcher is using an untested measure to conduct their study. For example, if the components of the IAMS framework are used without validation, a model and a system developed based on the framework would need to be revised, and another round of pilot study must be conducted. On the other hand, if the components were validated early on, any model or system developed based on the framework would require less revision, and need not be evaluated repeatedly.

Figure 2 clarifies an overview of the expert evaluation process for the IAMS framework. The diagram shows four main parts. The following sections will explain in detail how the expert evaluation was developed, as well as how the validation of content study was conducted.

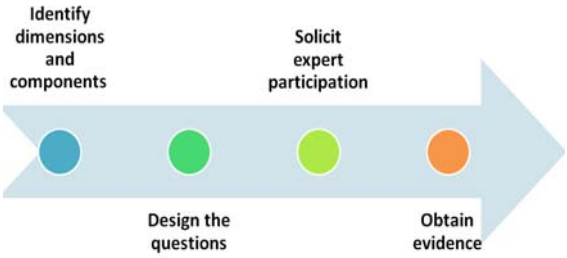

Figure 2. Development of the expert evaluation measuring instrument

5.1. Identify Dimensions and Components

Using the IAMS framework as a source of reference and guide, three dimensions were selected for inclusion in measuring experts' agreement on the components of integrating physical and virtual identity access management systems, which are: (1) Security and identity, (2) Acceptability and accessibility, and (3) User experience and usability. For each dimension selected, the appropriate components were selected for inclusion in the

measuring instrument. A total of 9 components (themes) were selected, with 3 components representing the Security and identity dimension, and 6 for Acceptability and User experience dimensions, as demonstrated in previous section.

5.2. Design the Questionnaire

The research questionnaire was formulated with the aim of measuring experts' agreement patterns concerning the components of the framework of integrating physical and virtual IAMSs. It constitutes a set of questions involving items and items' descriptions, and has been made available online[1]. A total of 60 items were created for the instrument with 15 items for the security dimension, 12 for the acceptance dimension, and 33 items for User experience dimension.

The questions used to evaluate the IAMS have adopted a Likert Scale. The Likert scale is a commonly used approach in questionnaires to measure participants' opinions and attitudes regarding a certain statement. The different scales are known as Likert items, and are used instead of numerical scales [29]. The response option adopts a four-point scale format, with the Likert items and their weights used in the questionnaire shown in Table 2.

Table 2. The Likert items and their weights

Opinion	Weight	Weighted Mean[2]	Definitions
Not Important	1	from 1.00 to 1.74	the exclusion of that item does not affect security in IAMS Framework
Somewhat Important	2	from 1.75 to 2.49	the exclusion of that item may need a revision in terms of wording or reorganization to make it more relevant to the framework.
Quite Important	3	from 2.50 to 3.24	
Very Important	4	from 3.25 to 4.00	the exclusion of that item would be important for security in IAMS Framework.

The emergence of IAMSs has only recently been witnessed, and thus the level of research and development in the respective field is limited. Moreover, although several research studies have been published around the world with focus on the integration of physical and virtual services, no research study conducted thus far has been found to include Security, User Experience, and Acceptability perspectives; therefore, the questionnaire should include a brief overview concerning the research and the current issues for each perspective. A video tutorial contains these data, which has been uploaded at the research's website[3]. The process of the questionnaire was structured as shown in Figure 3:

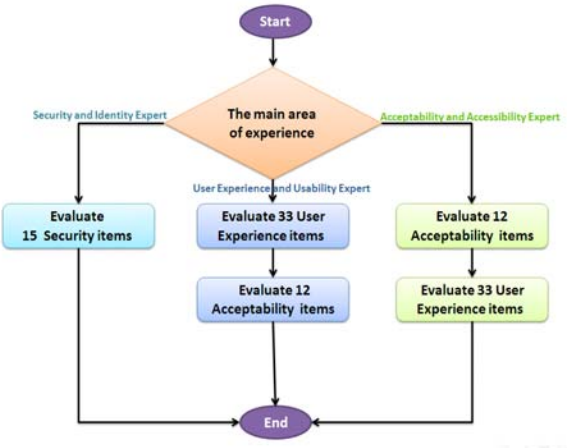

Figure 3. Questionnaire's steps Flowchart

As shown in Figure 3, a question is posed concerning the main area of experience of the participant to establish their experience in relation to the research study's criteria:

1. If the participant selects 'Security and Identity', then just the list of questions in regard to 15 security and identity items will be asked.
2. If the participant selects 'Acceptability and Accessibility', the list of 12 questions regarding the Acceptability and Accessibility items will be shown. Subsequently, because there is an 'Effective Operability' theme and set of items related to both Acceptability and User Experience dimensions, the list of 33 User Experience questions will be posed to the Acceptability Experts.
3. If the participant selects 'User Experience and Usability', the list of 33 questions regarding User Experience items will be shown. Following, the list of 12 questions regarding the Acceptability and Accessibility items will be asked since there are items between these dimensions.

5.3. Solicit Expert Participation

"The content validity of the questionnaire items may be examined by using an expert panel" [30], who will evaluate individual items, as well as the entire framework [28]. Rubio et al. suggest that the choice of expert depends on their knowledge, history of publications, presentations, and research experience in regard to the conceptual framework [28]. For example, the purpose of this research is to evaluate the IAMS framework; therefore, panel members should be familiar with one of the three

[1] At the following URL: https://qtrial.qualtrics.com/SE/?SID=SV_abpqFsjFHZ2RpTC

[2] It is important to weigh the Likert items according to a specific scale so that the answers of the participants can be measured. The range in each scale is approximately (3/4~ 0.75), and has been calculated according to the length between these four digits (1--2--3--4).

[3] www.fingerid.me/word/?page_id=8

research dimensions and/or have experience and familiarity in IAMSs. Rubio et al. recommend having two types of experts in the panel: (1) Lay Experts, who are people "for whom the topic is most salient… they help to address issues such as phrasing and unclear terms and recommends other important or significant items" [28]; and (2) Content Experts, who are "professionals and have published or worked in the field" [28]. Therefore, a sample of 9 Lay Experts (3 experts for each dimension) were selected, all of whom are postgraduates or researchers at the Electronics and Computer Science School at the University of Southampton, and have had experiences in one of the research dimensions. There were 5 females and 4 males, ranging in age between 20 and 50 years. Importantly, the sample members were recruited based on their interest in the research perspectives. Furthermore, the number of Content Experts were selected to use in a content-validity study ranging from five to a panel of fifteen experts for each dimension. All experts from this category have more than ten years' experience, are authors of published articles and books, and are also well known in the arenas of security, accessibility or usability, particularly in Access Management Systems.

5.3.1. Informal pilot study. This step was implemented in an attempt to garner comments and recommendations from lay experts concerning the questionnaire design, and to further ensure the content experts reading the item were able to understand what the item represents in the context of each dimension. After meeting each lay expert individually, comments were provided, with some items recommended for deletion, and the phrasing of some items highlighted as being unclear. After taking their feedback and making the necessary changes, a total of 52 items were created for the instrument, with 13 items for the security dimension, 10 items for the acceptance dimension, and 29 items for the User Experience dimension.

5.3.2. An invitation email to solicit experts participation. After conduction an evaluation using the lay experts, an invitation email requesting content experts' participation was sent a week before the actual start of the study; this allowed enough time for the individuals to respond to the request. The invitation email included a cover letter detailing the purpose of study, the reason the expert was selected, a description of the measure and its scoring, and an explanation of the response form, and a link to the research website, notably containing a brief about the study and a video tutorial. The samples were informed that their participation was voluntary, and that all data were completely anonymous and confidential. The study was on-going for three weeks.

5.4. Obtain evidence

Of the 45 experts, 28 experts returned the survey with data; 11 were the Security experts, 9 were Acceptability experts, and 8 were User Experience experts. The User Experience experts asked the Acceptability questions as well as the User experience questions as the User experience items are related to Acceptability items. Moreover, Acceptability experts were asked to rate the User experience items for the same reason.

Data screening was carried out with the aim of checking for reverse coding and any missing data. No items were reverse-coded, and no data was found to be missing. The distribution of most items in the three research perspectives, and the total of these items, are approximated as normal.

There is the use of the One Sample T-Test procedure with the objective to determine the mean of the level of agreements amongst respondents in regard to the items in the three research perspectives. This test helps to find out if each item is in important side or not for keeping and deleting these items by establishing whether or not the means of these items are smaller than 2.49. Figure 4 below shows the two sides according to weight means.

Figure 4. The two sides according to weight means

This test involves testing the null hypothesis[4] H0: $\mu=\mu 0$ against the alternative hypothesis[5], H1: $\mu\neq\mu 0$. The hypotheses established for testing each item in the three research perspectives are as follows:

- *The null hypothesis (H0):* There is no significant difference between the sample mean and the population mean; thus, the level of agreements relating to each research perspective's item is equal to 2.49.
- *The alternative hypothesis (H1):* There is a significant difference between the sample mean and the population mean; thus, the level of agreements relating to each research perspective's item is not equal to 2.49.

To make such a decision, the significance level, α (alpha), with a typical value of 0.05, is chosen. Then:

[4] The null hypothesis, H0, refers to a theory that has been stated. The reason of this statement is either that it is assumed to be correct or that it is needed as a base for argument, but has not been proved.

[5] The alternative hypothesis, H1, is a statement of what a statistical hypothesis test will be aiming to prove

- if Sig. (for each item) is less than or equal to α , reject H0; or
- if Sig. (for each item) is greater than α , reject H1.

5.4.1. Security and Identity Experts' Results. Table 3 summarises the descriptive statistics results, as well as the results of the One Sample T-Test. As shown, the significance value (Sig.) for all items—except Item 7—is less than 0.05 ($p<.05$); therefore, the researchers reject the null hypothesis (H0) and instead accept the alternative hypothesis (H1) for all items with the exception of Item 7. Moreover, the means of all the items, except Item 7, are significantly greater than the population mean since $\mu 0 = 2.49$; thus, all items, except Item 7 are important security items within the IAMS framework. Notably, however, the significance value of Item 7 is .518, which is more than 0.05. As such, the researchers reject the alternative hypothesis (H1) and accept the null hypothesis (H0). Accordingly, the security experts recommend the removal of Item 7 from the IAMS framework.

Table 3. One-Sample Test and Statistics for Security items

Items	Sig.	Mean	Attitude	Accepted Hypothesis
item 1	.000	3.18	Quite Important	Alternative
item 2	.012	3.18	Quite Important	Alternative
item 3	.025	3.18	Quite Important	Alternative
item 4	.008	3.27	Very Important	Alternative
item 5	.003	3.45	Very Important	Alternative
item 6	.002	3.36	Very Important	Alternative
item 7	.548	2.36	Somewhat Important	Null
item 8	.000	3.73	Very Important	Alternative
item 9	.002	3.36	Very Important	Alternative
item 10	.000	3.36	Very Important	Alternative
item 11	.002	3.36	Very Important	Alternative
item 12	.000	3.64	Very Important	Alternative
item 13	.001	3.45	Very Important	Alternative

5.4.2.Acceptability and Accessibility' Results. Table 4 clarifies the descriptive statistics and One Sample T-Test's results for acceptability and accessibility's experts, who evaluated 10 acceptability's items (starting from Item 14 up to Item 23). Moreover, the experts evaluated 29 User Experience items (starting with Item 24 and running up to Item 52). The results of the evaluation are given in Table 5. It is clear in both tables that the significance value (Sig.) for all items is less than 0.05 ($p<.05$); therefore, the researchers reject the null hypothesis (H0) and instead accept the alternative hypothesis (H1) for all items. In addition, the means of all items is considerably greater than 2.49; thus, all items are on the important side in the IAMS framework.

Table 4. One-Sample Test and Statistics for Acceptability items from Acceptability's Experts

Items	Sig.	Mean	Attitude	Accepted Hypothesis
Item 14	.007	3.33	Very Important	Alternative
Item 15	.002	3.56	Very Important	Alternative
Item 16	.001	3.67	Very Important	Alternative
Item 17	.054	3.22	Quite Important	Alternative
Item 18	.004	3.44	Very Important	Alternative
Item 19	.000	3.67	Very Important	Alternative
Item 20	.000	3.56	Very Important	Alternative
Item 21	.001	3.67	Very Important	Alternative
Item 22	.002	3.56	Very Important	Alternative
Item 23	.001	3.67	Very Important	Alternative

Table 5. One-Sample Test and Statistics for User Experience items from Acceptability's Experts

Items	Sig.	Mean	Attitude	Accepted Hypothesis
UX Item 24	.007	3.33	Very Important	Alternative
UX Item 25	.004	3.44	Very Important	Alternative
UX Item 26	.000	3.67	Very Important	Alternative
UX Item 27	.000	3.56	Very Important	Alternative
UX Item 28	.004	3.44	Very Important	Alternative
UX Item 29	.000	3.56	Very Important	Alternative
UX Item 30	.004	3.44	Very Important	Alternative
UX Item 31	.000	3.78	Very Important	Alternative
UX Item 32	.000	3.56	Very Important	Alternative
UX Item 33	.000	3.67	Very Important	Alternative
UX Item 34	.007	3.33	Very Important	Alternative
UX Item 35	.002	3.56	Very Important	Alternative
UX Item 36	.004	3.44	Very Important	Alternative
UX Item 37	.022	3.44	Very Important	Alternative
UX Item 38	.004	3.44	Very Important	Alternative
UX Item 39	.001	3.67	Very Important	Alternative
UX Item 40	.004	3.44	Very Important	Alternative
UX Item 41	.004	3.44	Very Important	Alternative
UX Item 42	.002	3.56	Very Important	Alternative
UX Item 43	.002	3.56	Very Important	Alternative
UX Item 44	.000	3.56	Very Important	Alternative
UX Item 45	.004	3.44	Very Important	Alternative
UX Item 46	.004	3.44	Very Important	Alternative
UX Item 47	.004	3.44	Very Important	Alternative
UX Item 48	.007	3.33	Very Important	Alternative
UX Item 49	.004	3.44	Very Important	Alternative
UX Item 50	.001	3.67	Very Important	Alternative
UX Item 51	.001	3.67	Very Important	Alternative
UX Item 52	.012	3.38	Very Important	Alternative

5.4.3.User Experience and Usability' Results. User Experience and Usability's experts evaluated the importance of 29 User Experience items and 10 Acceptability items in the IAMS framework. Table 6 and Table 7 explain the descriptive statistics and One Sample T-Test's results for 29 User Experience items (starting from Item 24 and running up to Item 52), and 10 Acceptability items (ranging Item 14–Item 23). It is clear in the case of both tables that the significance value (Sig.) for all items is less than 0.05 ($p <.05$); therefore, the researchers reject the null hypothesis (H0) and accept the alternative hypothesis (H1) for all items. In addition, the means of all items is noticeably more than 2.49; thus, User Experience experts find all items to be on the

important side, with all needing to be kept in the IAMS framework.

Table 6. One-Sample Test and Statistics for User Experience items from User Experience's Experts

Items	Sig.	Mean	Attitude	Accepted Hypothesis
UX Item 24	.046	3.25	Very Important	Alternative
UX Item 25	.026	3.13	Quite Important	Alternative
UX Item 26	.012	3.38	Very Important	Alternative
UX Item 27	.001	3.50	Very Important	Alternative
UX Item 28	.026	3.13	Quite Important	Alternative
UX Item 29	.002	3.25	Very Important	Alternative
UX Item 30	.019	3.25	Very Important	Alternative
UX Item 31	.000	3.63	Very Important	Alternative
UX Item 32	.000	3.75	Very Important	Alternative
UX Item 33	.012	3.38	Very Important	Alternative
UX Item 34	.002	3.38	Very Important	Alternative
UX Item 35	.000	3.63	Very Important	Alternative
UX Item 36	.012	3.38	Very Important	Alternative
UX Item 37	.000	3.63	Very Important	Alternative
UX Item 38	.002	3.25	Very Important	Alternative
UX Item 39	.000	3.88	Very Important	Alternative
UX Item 40	.000	3.63	Very Important	Alternative
UX Item 41	.001	3.50	Very Important	Alternative
UX Item 42	.000	3.75	Very Important	Alternative
UX Item 43	.002	3.25	Very Important	Alternative
UX Item 44	.001	3.50	Very Important	Alternative
UX Item 45	.000	3.75	Very Important	Alternative
UX Item 46	.001	3.50	Very Important	Alternative
UX Item 47	.002	3.38	Very Important	Alternative
UX Item 48	.000	3.75	Very Important	Alternative
UX Item 49	.000	3.75	Very Important	Alternative
UX Item 50	.002	3.25	Very Important	Alternative
UX Item 51	.000	3.63	Very Important	Alternative
UX Item 52	.000	3.75	Very Important	Alternative

Table 7. One-Sample Test and Statistics for Acceptability items from User Experience's Experts

Items	Sig.	Mean	Attitude	Accepted Hypothesis
Item 14	.001	3.13	Quite Important	Alternative
Item 15	.007	3.50	Very Important	Alternative
Item 16	.002	3.25	Very Important	Alternative
Item 17	.002	3.38	Very Important	Alternative
Item 18	.002	3.38	Very Important	Alternative
Item 19	.001	3.50	Very Important	Alternative
Item 20	.001	3.13	Quite Important	Alternative
Item 21	.046	3.25	Very Important	Alternative
Item 22	.012	3.38	Very Important	Alternative
Item 23	.001	3.50	Very Important	Alternative

6. Summary and Conclusion

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.

An expert evaluation study was conducted with 11 security experts, 9 acceptability experts, and 8 user experience experts from both academic researchers and professional designers. Results suggest that there is a statistical significance between the experts' agreement on the components/attributes of the IAMS framework. Although the security experts' results suggest the removal of Item 7, 'Authority of the user to disclose data with a desired information flow', from the IAMS framework, 'Control of Information' attribute/component, which contains Item 7, will be kept in the IAMS framework as it comprises two very important items, namely Item 6 and Item 8. Therefore, these findings provided evidence that the IAMS framework is based on sound theoretical foundations from research in regard to all three research perspectives.

7. 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.

[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.

[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.

[12] Alotaibi, Sara Jeza and Wald, Mike (2012). Security, User Experience, Acceptability Attributes for the Integration of Physical and Virtual Identity Access Management Systems In, *The IEEE International Conference on Information Society (i-Society 2012),* London, UK, 25 - 28 June 2012.

[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.

[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] 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)*

[20] 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)

[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] 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)*

[23] 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)*

[24] 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)*

[25] 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)*

[26] Alotaibi, Sara Jeza and Wald, Mike (2012). IAMS Framework: A New Framework for Acceptable User Experiences for Integrating Physical and Virtual Identity Access Management Systems In, *The IEEE World Congress on Internet Security (WorldCIS-2012), Ontario, Canada, 10 - 12 June 2012.*

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

[28] Rubio, D. M., Berg-Weger, M., Tebb, S. S., Lee, E. S., & Rauch, S. (2003). Objectifying content validity: Conducting a content validity study in social work research. *Social Work Research*, *27*(2), 94-104.

[29] Lankes, D. (2002). Building a Successful Customer-service Culture: A guide for Library and Information Managers. *Library Association Publishing: London, UK.*

[30] Saw, S. M., & Ng, T. P. (2001). The Design and Assessmement of Questionnaires in Clinical Research. *Singapore medical journal*, *42*(3), 131-135.

