Published in the proceedings of the International Conference on High Performance Computing and Simulation (HPCS), 2012

A Comparative Analysis of Identity Management Systems

Md. Sadek Ferdous
School of Computing Science,
University of Glasgow, Glasgow, Scotland
E-mail: m.ferdous.1@research.gla.ac.uk

Ron Poet
School of Computing Science,
University of Glasgow, Glasgow, Scotland
E-mail: ron@dcs.gla.ac.uk

***Abstract*— In this paper, we present a comparative analysis of a few popular Identity Management Systems against a set of requirements. Identity Management and Identity Management Systems have gained significant attention in recent years with the proliferation of different web-enabled and e-commerce services leading to an extensive research on the field in the form of several projects producing many standards, prototypes and application models both in the academia and the industry. We have collected and compiled different requirements from different sources to profile an extensive set of requirements that are required for a Privacy-Enhancing Identity Management System and presented them in the form of a taxonomy. Then we have compared some Identity Management Systems against those requirements and presented them in a concise way to help readers find out instantly which systems satisfy what requirements and thus help them to choose the correct one to fit into their own scenarios.**

Keywords- Identity Management; Identity Management Systems; Security; Privacy; Privacy Enhancing Technologies

I. INTRODUCTION

Currently there are literally thousands of websites around the world providing a plethora of different services via the Internet. These services require that users present their identities for authentication in case they want to access those services. To manage different users with their identities, Identity Management (IdM, in short) was introduced initially by the industry to facilitate online management of user identities. Different research initiatives led to the creation of different models and prototypes of Identity Management Systems with each system satisfying its own sets of requirements. Identifying what requirements are served by which systems can be very challenging since the requirements served by different IdM Systems are written in their respective specifications and scattered among several documents. This paper aims to aid in this regard by presenting a comparison among different leading Identity Systems a concise way so that any reader can instantly deduce which requirements are fulfilled by those IdM Systems and which are not.

That said, this paper is organised as follows. We discuss the related works in Section 2. In Section 3, we briefly describe our chosen Identity Management Systems. We present a taxonomy of requirements for an ideal Identity Management System and provide a brief description of each requirement in Section 4. We present our result of comparison among the selected systems against that set of requirements in tabular formats as well as discuss our findings and the limitation and strength of our analysis in Section 5. Finally, we conclude in Section 6.

II. RELATED WORK

There are many Identity Management Systems currently available. Requirements for each such system are usually published in their respective specifications, documentations, wiki pages, webpages or published papers. Several efforts to converge those requirements from different sources can be found in [1], [2], [3], [4] and [5]. We have extended their works by adding a very few new requirements, subtracting some and then restructuring several requirements so that a concise taxonomy can be built.

A couple of examples for analysing existing Identity Management Systems using a set of criteria can be found in [2] and [3]. A few Identity Management Systems such as Microsoft .NET Passport, Liberty Alliance Architecture, Novell DigitalMe, etc. and applications such as Mozilla 1.4 Navigator, Microsoft Outlook Express 6 SP1, CookieCooker, etc. were analysed against a set of requirements. In current settings, their work is almost outdated in the sense that many of those systems are either functional in a restrictive way or have been evolved into something new (e.g. Novell DigitalMe transformed to the Bandit Project [6]). A more recent attempt with the same objective can be found in [3] in which four Identity Management Systems – Liberty Alliance Architecture, Shibboleth, PRIME Architecture and Microsoft CardSpace have been analysed against a set of requirements. However, the current work provides the following improvements over those works:

1. Our work provides and explains a comprehensive taxonomy of requirements for an ideal Identity Management in a more systematic way than any previous works.
2. Our work has compared 6 leading Identity Systems which is 50% more than that of the last work.
3. Our work is more elaborative in the sense that the number of requirements that were considered previously is far less than that of this current work.

4. Moreover, our work is much more concise (327 pages in [2] and 76 pages in [3]). Previous findings were published in a descriptive way and readers would need to read through a lengthy document to identify the missing features. We have presented our findings in a tabular format which is more illustrative and believe that it will allow any reader to instantly identify which requirements are met by which systems.

III. Selected Identity Management Systems

We have chosen six Identity Management Systems for our comparative analysis which either have dominant positions in Identity Management scenarios or introduced a novel concept which is worth exploring.

A. Windows CardSpace

It was envisioned by Microsoft that an Identity Metasystem - a system of systems - which is application agnostic and can accommodate all existing technologies in a standard way can provide a better solution to reduce many of Identity Management problems. Windows CardSpace is their developed Identity Metasystem [7]. Unfortunately, Microsoft has discontinued their CardSpace project. However, we have opted to include it into our analysis because of its fundamentally novel concept of Identity Metasystem. A brief introduction to Windows CardSpace can be found in [8].

B. OpenID

OpenID is a decentralised Identity Management System which provides SSO solution for web services over the Internet [9]. It is a User-Centric technology and is being used by many web service providers such as AOL, BBC, Google, IBM, MySpace, Orange, PayPal, Verisign, LiveJournal, Yahoo, etc. [10], [11]. With more than 1 billion OpenID enabled accounts and 9 million OpenID-enabled websites OpenID is one of the wide-spread IdM Systems with huge user-bases [11] and that is why it has been chosen for the analysis. A brief introduction to OpenID can be found in [12].

C. Shibboleth

Shibboleth is an open-source, provider-centric Federated Identity Management middleware initiative by the Internet2 consortium and based on Security Assertion Markup Language (SAML) standard [13]. It is another widely adopted leading Federated Identity Management System especially in the Academia and that is why it has been chosen in this paper. A brief introduction on Shibboleth Architecture can be found in [14].

D. Liberty Alliance Architecture

Liberty Alliance (LA, in short), established in 2001 and currently known as Kantara Initiative, is a consortium of commercial and non-commercial organisations aiming to develop and provide open and interoperable standards for Federated Identity Management [15]. It has produced a number of non-normative specifications to enable a secure and privacy-friendly identity-enabled products and services mainly based on SAML. A brief introduction regarding the LA Architecture can be found in [16].

E. PRIME Architecture

The PRIME (Privacy and Identity Management for Europe) Project was an EU and Swiss Government funded project under FP6 Framework and was aimed to pursue research on how to integrate different technical and non-technical issues of Privacy Enhancing Technologies (PETs) with the Identity Management scenarios and then to design and develop prototypes of privacy-enhancing Identity Management Systems [17]. The result was the PRIME Architecture which has strong focus on privacy. PRIME Architecture has been explained in details in [18].

F. OAuth

OAuth is one of the fastest growing community-based specifications and has been designed to circumvent the limitation of the delegation in the traditional service model [19]. The original specification, known as OAuth 1.0, was finalised in April 2010 and is specified in RFC 5849 [20]. However, it went through a complete modification and evolved to a new version called OAuth 2.0 is be finalised this year [21].

IV. Taxonomy of Requirements

In this section we explain each requirement very briefly. The requirements have been structured in the form a taxonomy (Fig. 1) so that they can be used as comparable metrics for comparing different systems.

A. Functional Requirements (FR)

The core services with respect to the Identity Management Systems fall into this category.

1) Identity Administration (IA)

This group includes those requirements that are required to administrate partial identities and other identity information.

a) Creating, updating and deleting Partial Identity and its related information (CrUD).

An Identity Management System should allow any user to create a new partial identity and then should offer the service to update and, if a user wants, delete her existing partial identity and identity information.

b) Usage of Pseudonyms (Psd)

To offer a better privacy, users should have the capability to choose when to release her original partial identity and when to use a Pseudonym. The Pseudonym should be unlinkable to the original partial identity and the system should offer the possibility of creating, updating and deleting different Pseudonyms.

c) Credential Management(CM).

Credential is an important part of authentication and authorisation; hence a system should have good credential management capability.

d) Identity Recovery (IR)

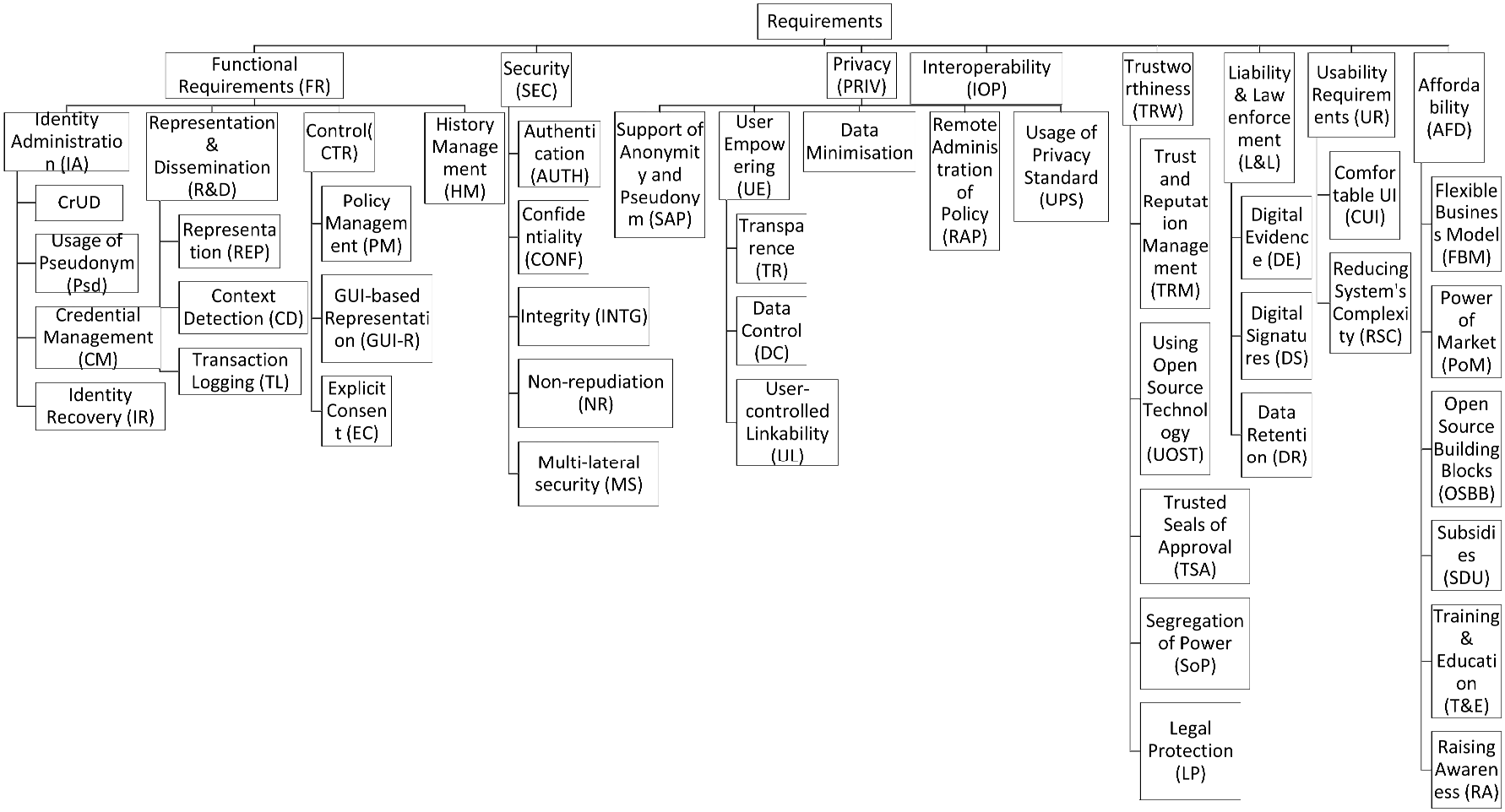

Figure 1. Taxonomy of Identity Management Requirements

Once a digital partial Identity has been stolen by an intruder it needs to be recovered as soon as possible, hence a system should specify an identity recovery mechanism.

2) Representation & Dissemination (R&D)

This group enlists those requirements that are required for representation and dissemination of identity data.

a) Representation (REP)

The effectiveness and usefulness of an IdM system largely depends on how the identity data is represented and visualised at the user-interface. It helps users to select and choose correct partial identities, pseudonyms and other attributes to be released to the communication partner for a specific service.

b) Context Detection(CD)

Context detection can help to minimise data release and thus can preserve privacy. Therefore, a system should have the ability to detect the context.

c) Transaction Logging (TL)

Each transaction using an IdM System should be logged for the purpose of history management.

3) Control (CTR)

This set of requirements allows users to control the data flow between the user and the communication parties which is essential for any User-centric approach as well as for preserving user-privacy.

a) Policy Management (PM)

An IdM System should offer users the control over the data flow by allowing users to choose the right profile/partial identity/pseudonym with related attributes for any given transaction. This can be effectively done using different policies. Therefore, an IdM system should have the ability to offer rule or policy management ability.

b) GUI-based Representation (GUI-R)

A standard GUI-Based representation should be used to help users to choose or create an appropriate partial identity or pseudonym for any given transaction. If the user selects an existing pseudonym, the GUI should inform the user which entities that pseudonym has been released to. This will help her to make an informed choice.

c) Explicit Consent (EC)

An IdM System should inform the user via an intuitive GUI about the data the system is releasing and ask for her explicit consent before any release.

4) History Management (HM)

A good history management facility should display all logged transactions in a user-friendly way. This will allow users to check their data trail, i.e. what partial identity/pseudonym and other attributes have been released to what entity, when they have been released, if there is any privacy policy attached to the released data, etc.

B. Security (SEC)

An IdM system can be used for accessing different services ranging from participating in social network activities, blogging and emailing to accessing Government services, online banking, e-commerce activities, etc. There are different levels of security for each of this service yet each activity requires a minimum security guarantee to make sure that only the authenticated user can access the requested service securely.

1) Basic Security Mechanisms: Authentication (AUTH), Confidentiality (CONF), Integrity (INTG) and Non-repudiation (NR).

The core mechanism of an IdM system is to ensure the authenticity of a user. For simple web services, this can be done using a user-id and password. For more secured services such as financial or Government services, biometrics, OTP (One-time password), hardware tokens, etc. could be used. Confidentiality is to ensure that the transmitted data between two parties is not disclosed to any unauthorised entity. Integrity is to ensure that the transmitted data is not altered during transmission. Non-repudiation ensures that a user, once committed for a transaction, cannot deny her commitment. Cryptographic mechanisms can be used to ensure Confidentiality, Integrity and Non-repudiation.

2) Multi-lateral security (MS)

When there are more than one party in an action, ensuring security for all of them is the theme of Multi-lateral security. An IdM system essentially involves more than one party and that is why it is especially important to consider the issue of multi-lateral security in IdM system. Multi-lateral security assumes that each party minimally trusts each other where each party can keep and enforce its own security goal [2].

C. Privacy (PRIV)

Currently, the privacy of a user, user identity and the identity information are very important. Privacy Enhancing Technologies (PETs) are the basic mechanism by which privacy can be guaranteed. Configuring an IdM with the principles of PET should ensure privacy protection mechanisms integrated into the technology. A list of such principles can be derived from [22]. We are enlisting only those requirements that can be used to ensure the privacy of a user in the IdM setting.

1) Support of Anonymity (ANON) and Pseudonym (SAP)

A Privacy-aware IdM System should have a strong support for Anonymity. Likewise, it should support the usage of Pseudonym to ensure that users are unlinkable at the SP when they want to do so. Privacy protection techniques using various cryptographic methods can be used to achieve these requirements.

2) User Empowering with Transparency (TR), Data Control (DC) & User-controlled Linkability (UL) (UE, for the whole property)

All the above mentioned privacy requirements will be in vain if users are not in control of their data and have no idea which data is released to which entity. We can empower the

user for managing their identities with the help of Transparency (to let users be aware of what sort of personal data is being transmitted to which entity and how they are stored and processed at different parties), controlling the data flow as well as with the ability to maintain a user-controlled linkability.

3) Data Minimisation (DM)

Data minimisation can ensure that only the required data is stored and processed at the SP and can guard against the release of unnecessary yet sensitive personal data to unauthorised parties which ultimately reduces the risk of privacy breach.

4) Remote Administration of User Policies (RAP)

In the traditional IdM System, users have no control over their data once it has been released to other parties. One way to enforce the control over released data is to allow users to administer their data remotely.

5) Usage of Privacy Standard (UPS)

The Platform for Privacy Preferences (P3P) Project is a W3C standard that allows websites to express their data collection and management policies to their visitors in a machine readable format [23]. Using a privacy standard such as P3P could allow users to express their privacy requirements in a standard way.

D. Interoperability (IOP)

It will be crucial for any IdM system to have a good degree of compatibility with other existing systems to make it a hugely successful one.

E. Trustworthiness (TRW)

Users need to trust an IdM system as they will need to provide a lot of their personal information. One the other hand, a successful IdM System needs to gain the user's trust to exist. In this section we are enlisting those factors that are required to build and maintain a mutual trust between a user and an IdM System.

1) Trust and Reputation Management (TRM)

In Multi-lateral scenarios like Identity Management, trust is one of the central issues as the parties involved need to trust each other in a certain way. This raises the question of how trust issues can be managed properly. Trust is a complex issue. There are so many different parameters and it takes time to gain trust. However, a better implementation and a good balance of usability, security and privacy could be a decisive factor for users to place their trust on an IdM system. Another related issue is the reputation of users in scenarios like Amazon or eBay. In such settings, reputation data is considered to be a personal data and therefore should be protected like any personally identifying data. Trust data are usually not of quantifying type and hence they cannot be used as a comparable metric. Therefore, we will not include it into our comparison.

2) Using Open Source Technology (UOST)

The use of open source technology helps to gain user trust. When the source code of a system is released, it can validate many of its security and privacy properties which in turn can increase its trustworthiness.

3) Trusted Seals of Approval (TSA)

Security and privacy seals sometimes can be used to assert that the system is secure or privacy-friendly according to a standard. An example of a security seal is the Verizone Certified to certify if a website is secure and an example of a privacy seal is the P3P Seal to attest that a website complies to the P3P Privacy policies.

4) Segregation of power (SoP)

Segregation of power is an important tool to gain trust among users especially in multi-lateral scenarios like Identity Management. Such property will ensure that no single entity will have dominant position over other entities so that it cannot abuse its power to monopolise a service. To enable the segregation, it is necessary that the identity eco-system and market itself is matured enough and users have the ability to choose a specific entity based on their performance.

5) Legal Protection (LP)

Legal protection is another way to achieve user-trust especially in situation where financial transactions are involved such as e-banking, e-auction, web-commerce, e-taxation, etc. When users find they are legally protected against attacks while using such services they will feel more comfortable to get involved in transaction which in turn increases the trustworthiness towards the system. Since the legal requirement depends on a specific country or place and the data cannot be quantified, we will not include it into our comparison.

F. Liability & Law enforcement (L&L).

Legal protection and ensuring liability is fundamentally important for widespread usage and reputation of an IdM system. The level and degree, again, depend on the context and scenario in which an action is taking place. That's why it should be adjustable by users who will fine tune the settings according to the scenarios they are involved in. Some requirements to ensure liability are given below.

1) Digital Evidence (DE)

Digital evidence can be used as the primary witnessing source and would be necessary to claim liability or legal protection in case of identity theft, reputation theft, warranty or wrong delivery, tax fraud, unauthorised access, civil action, etc. The mechanisms and how they can be integrated into an IdM system are still an open issue and needs to be further explored.

2) Digital Signatures (DS)

Digital signature is the ultimate tool to ensure non-repudiation especially in financial and citizen services. It should be used when there is any chance of dispute, especially in highly sensitive data transaction.

3) Data Retention (DR)

Data retention is the policy by which an organisation can archive persistent data securely and in a privacy-friendly way. It can be used in case any dispute arises. However, this is opposite to the requirements of data minimisation which states to store only the minimum amount of personal data.

How to find a good balance between these two is still an open question.

G. Usability Requirements (UR).

Usability of a system determines not only the usefulness of a system but also ensures the effectiveness of the security mechanism. A usable system is easily adaptable and increases the effectiveness of a system.

1) Comfortable UI (CUI)

User-interface is the primary point for users to get involved with the system. It is the central component that allows users to ensue transaction, set privacy policy, give explicit consent and check the data trail via the history functionality, therefore it must host an intuitive, comfortable and easy to use UI.

2) Reducing System's Complexity (RSC)

A simply-presented system will less likely confuse a user than a complex system. A system may be very complex in nature. However, it is wise to hide this complexity from the user with a simple and intuitive UI. Since there is no way to quantify this requirement, it will not be used as a comparable metric.

H. Affordability (AFD)

As a general rule, the integration of an IdM system should not be more expensive than the actual transaction; otherwise it will drive the users away. It might be advantageous if a new IdM system could bring in additional advantages by creating the possibility for new business model and/or services. In this group, we are enlisting those requirements that would be helpful for any new IdM System to get wide-spread adoption.

1) Flexible Business Model (FBM)

A flexible yet attractive business model for any IdM System is one of the essential properties to gain wide-spread adoption. Other than users, an IdM System usually interacts with business organisations. Therefore, a new IdM System has to offer a substantial amount of incentives before any organisation decides to get involved with the IdM System. Since there is no way to quantify this requirement, it will not be used as a comparable metric.

2) Power of Market (PoM)

The success of an IdM system ultimately depends on the diversity of service it provides, the ease of availing those services and the value-for-money for each service. Therefore, the market that provides different services should be a matured one with optimal cohesion between different entities.

3) Open Source Building Blocks (OSBB)

This will not only enable to reduce the production as well as adoption cost for an IdM system as well as help to gain user-trust. The analysis of this requirement will be same as the UOST requirement.

4) Subsidies for Development, Use, Operation, etc. (SDU)

Government can provide subsidies for development, use, operation, etc. for an IdM system in case it is in line with the Governmental aims and objectives. Since there is no way to quantify this requirement, it will not be used as a comparable metric and therefore we will not use it for comparsing the systems.

5) Training and Education (T&E)

Training and education can be an effective way to educate users to use the system effectively. This is especially true for a new system when users are not familiar with the UI and functionalities.

6) Raising Awareness (RA)

Raising awareness helps people to be informed about the possible attack scenarios that can be launched against an IdM system or their identity data. This will help users to decide if a particular action is invading her security and privacy.

I. Comparison

We used the taxonomy of requirements listed above to compare the selected Identity Management systems. To compare them properly, we had to understand their inner architectures and familiarise ourselves with their protocols. Then we checked, one-by-one, if a single requirement was met by a system. For this, we had to consult their protocol descriptions, specification documents, corresponding wiki-pages and sometimes development forums. We now present our findings in Table I, II and III.

We have used the tick (√) mark, sometimes accompanied with an explanation in brackets (), to indicate that an IdM Systems satisfies a respective requirement and the character 'x' to indicate that the system does not satisfy the respective requirement. However, there is one exception in T&E column of the AFD requirement in Table 3, where tick (√) sign has used to indicate if the user of the respective IdM system would require any training and education to use it properly. The dash (-) character has been used in cases where the requirement is not of quantifying nature or a single '√' or 'x' is not enough to explain the analysis precisely. Another point of clarification would be the usage of a '-' for LA has been used to indicate that being just a specification it has been difficult to find the user-base of using any implementation of it and a '-' for PRIME has been used to indicate that being used by just a few prototypes which were developed as a proof of concept, it is very unlikely to have any reasonable number of users in the case of PoM under AFD requirement in Table III. Additionally, a 'Large User Base' for a discontinued system like CardSpace is used to indicate that being a part of the Windows family CardSpace is very likely to be already available to a large number of users. In another non-functional requirement, Comfortable UI (CUI), a (√) mark has been used to indicate that this requirement was considered while designing and developing the system and a (x) sign was used to indicate that the requirement was completely ignored in the specification and thereby not considered while developing the system.

As evident from the tables, excluding the entries with a '-', PRIME has met the maximum number of requirements (29 out of 33) and is followed by CardSpace (22 out 33), Shibboleth (18 out 33), OAuth (18 out of 33), OpenID (15 out 33) and LA being the last one (11 out of 33). Other than that, we can

TABLE I. FUNCTIONAL REQUIREMENTS

	FR										
	IA				R&D			CTR			HM
	CrUD	Psd	CM	IR	REP	CD	TL	PM	GUI-R	EC	
CardSpace	√ (InfoCard)	√ (Self-managed card)	X (IdP Specific).	√ (InfoCard Revocation)	√ (InfoCard)	√	√	√	√	√	√
OpenID	√ (URL/XRI)	X	X (Provider Specific)	X (Provider Specific)	√ (URL/XRI)	X	X	X	√	X	X
Shibboleth	X (IdP Spec.)	√	X (IdP Spec.)	X (IdP Specific)	√ (Supports different formats)	X	√	√	X (IdP Spec.)	√ (VIA ARP)	√
LA	X (IdP Spec.)	√	X (IdP Spec.)	X (IdP Specific)	√ (Supports different formats)	X	X	X	X (IdP Spec.)	√	X
PRIME	√	√	√ (Supports different formats)	X	√ (Supports different formats)	√	√	√	√	√	√
OAuth	X (IdP Spec.)	√	X (IdP Spec.)	X (IdP Spec.)	√	X	X	X	X	√	X

TABLE II. SECURITY, PRIVACY, INTEROPERABILITY & TRUSTWORTHINESS REQUIREMENTS

	SEC		PRIV								IOP	TRW	
	Basic Requirements (AUTH+CONF+ INTG+NR)	MS	SAP		UE			DM	RA	UPS		TRM	
			ANON	Psd	TR	DC	UL					TRUST	REPU
CardSpace	√	√	X	√ (Self-issued card)	√	√	X	√	X	X	√	-	-
OpenID	√	√	X	X	√	√	X	√	X	X	X	-	-
Shibboleth	√	√	X	√	√	√	X	√	X	X	X	-	-
LA	√	√	X	√	√	√	X	√	X	X	X	-	-
PRIME	√	√	√	√	√	√	√	√	√	√	√	-	-
OAuth	√	√	√	√	√	√	√	√	X	X	√	-	-

TABLE III. TRUSTWORTHINESS, LIABILITY & LAW-ENFORCEMENT, USABILITY & AFFORDABILITY REQUIREMENTS

	TRW				L&L			UR		AFD					
	UOST	TSA	SoP	LP	DE	DS	DR	CUI	RSC	FBM	PoM	OSBB	SDU	T&E	RA
CardSpace	X	X	X	-	X	√	X	√	-	-	Large User Base	X	-	√	√
OpenID	√	X	√	-	X	√	X	X	-	-	Large User Base	√	-	√	√
Shibboleth	√	X	X	-	X	√	X	X	-	-	Large User Base	√	-	√	√
LA	-	X	X	-	X	√	X	X	-	-	-	-	-	√	X
PRIME	X	√	√	-	√	√	√	√	-	-	-	X	-	√	√
OAuth	√	X	√	-	X	√	X	X	-	-	Large User Base	√	-	√	X

interpret our findings presented in the tables in a number of ways. We present here just a very few of them.

- With strong support for PETs, PRIME would have been the ideal choice among them for a privacy-enhancing Identity Management System. However, being only a research project with a very few prototypes, it is uncertain currently how it will be adopted in web-service scenarios. The second suitable choice CardSpace being discontinued, Shibboleth would be, presumably, the ideal choice in this regard.
- Each Identity Management System has somewhat good support for Security. However, many of them fail substantially to meet many privacy requirements. Therefore, it would be an interesting research topic to investigate the ways many privacy requirements can be integrated into those IdM Systems, especially, being the two leading IdM Systems, in OAuth and Shibboleth.
- Graphically and functionality-wise, CardSpace is the most feature-intensive. If otherwise missing privacy requirements could be integrated, it would have been the best choice for any circumstances.
- Context detection is another important requirement that has been missing in most current IdM Systems. Context detection could play a crucial role not only in data minimisation but also in Mobile Identity Management System where specific identity could be used based on the environment the user is currently in. Policy Management plays a major role in detecting context. Therefore, finding the interplay between the context detection and policy

management and how these can be easily integrated into the current Identity Management Systems could be another interesting research topic.

- Presenting partial identity using InfoCard like in CardSpace could be a viable candidate for managing identities in mobile devices and again an interesting research question. Google Wallet has already adopted a very similar approach [24].
- It would be also useful to keep in mind that some requirements, for example, functional, security and privacy requirements comprise the core set of requirements and carry more weights than others. Therefore, a system satisfying more of these requirements should be considered a better system than a system satisfying less of these core requirements even though the first system may satisfy less number of total requirements than the second system.

A. Limitations

The above tables present a simple way of illustrating the strengths and weaknesses of each Identity System and hence identifying gaps in Identity Architectures. However, the over-simplicity of the tabular format may obscure certain elements. For example, the tables cannot be used to identify the implementation of which system for a few type of requirements is better than that of others in case all systems satisfy those requirements. On the contrary, the tables would perform flawlessly for identifying weaknesses for any requirement.

II. CONCLUSIONS

In this paper, we have analysed a few Identity Management Systems against a set of requirements. We wanted to investigate if the selected systems meet these requirements and then present our findings in a tabular format so that any reader can easily identify the strengths and weaknesses of those systems. We have found that none of our selected Identity Management Systems (a few of them are actually the leading ones) can be declared as the ideal one which are functionally rich, privacy-preserving yet usable. Especially the lacking of different privacy requirements is worrisome. We have presented a very few interpretations of our findings as well as indicated some possible research directions based on our findings.

REFERENCES

[1] Future of Identity in the Information Society (FIDIS) Project WP3, "Study on Mobile Identity Management," May 2005. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.3.study_on_ mobile_identity_management.pdf

[2] "Identity Management Systems (IMS): Identification and Comparison Study," September 2003. https://www.datenschutzzentrum.de/idmanage/study/ICPP_SNG_IMS-Study.pdf

[3] Stefanie Pötzsch, Martin Meints, Bart Priem, Ronald Leenes and Rani Husseiki, "D3.12: Federated Identity Management – what's in it for the citizen/customer?" 10 June 2009. http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables/fidis-wp3-del3.12.Federated_Identity _Management.pdf

[4] Stefanie Pötzsch, Katrin Borcea-Pfitzmann, Marit Hansen, Katja Liesebach, Andreas Pfitzmann and Sandra Steinbrecher, "Requirements for Identity Management from the Perspective of Multilateral Interactions." in Jan Camenisch, Ronald Leenes, and Dieter Sommer, editors, *Digital Privacy*, volume 6545 of Lecture Notes in Computer Science, pages 609–626. Springer Berlin / Heidelberg, 2011. 10.1007/978-3-642-19050-6 22

[5] Tobias Kölsch, Jan Zibuschka, and Kai Rannenberg, "Digital privacy. Chapter: Privacy and Identity Management Requirements: An Application Prototype Perspective," pages 735–749. Springer-Verlag, Berlin, Heidelberg, 2011

[6] Bandit Project. http://code.bandit-project.org/trac

[7] Microsoft Windows CardSpace. http://www.microsoft.com/windows/products/winfamily/ cardspace/default.mspx

[8] David Chappell, "Introducing Windows CardSpace," April 2006. http://msdn.microsoft.com /en-us/library/aa480189.aspx

[9] OpenID Foundation Website. http://openid.net/

[10] Wikipedia entry on OpenID. Accessed on 2 September 2011. http://en.wikipedia.org/ wiki/OpenID

[11] Brian Kissel, "OpenID 2009 Year in Review," 16 December 2009. http://openid.net/2009/12 /16/openid-2009-year-in-review/

[12] OpenID Presentations. http://openid.net/community/presentations/

[13] Shibboleth. http://shibboleth.internet2.edu/

[14] Shibboleth Wiki. Accessed on 11 October 2011. https://wiki.shibboleth.net/confluence/display/SHIB2/UnderstandingShibboleth

[15] Liberty Alliance Project. http://www.projectliberty.org/

[16] Liberty Alliance Project: Liberty ID-FF Architecture Overview Version: 1.2-errata-v1.0. http://projectliberty.org/liberty/content/download/318/2366/file/draft-liberty-idff-arch-overview-1.2-errata-v1.0.pdf

[17] PRIME Project. https://www.prime-project.eu/

[18] "WP 14.2. PRIME Architecture V2," 29 March 2007. https://www.prime-project.eu/prime_products/reports/arch/pub_del_D14.2.c_ec_WP14.2_v1_Final.pdf

[19] oAuth Community Site. http://oauth.net/.

[20] Eran Hammer-Lahav, "The OAuth 1.0 Protocol – RFC," April, 2010. http://tools.ietf.org/html/rfc5849

[21] Eran Hammer-Lahav, "Introducing OAuth 2.0," 15 May 2010. http://hueniverse.com/2010/05/introducing-oauth-2-0

[22] Marit Hansen, "Privacy-enhancing technologies," Alexander Roßsnagel (Ed.): *Handbuch Daten-schutzrecht*; Verlag C.H. Beck, pages 291–324, München 2003.

[23] The Platform for Privacy Preferences (P3P) Project. http://www.ws3.org/P3P/

[24] Google Wallet. http://www.google.com/wallet