A survey of trust issues constraining the growth of Identity Management-as-a-Service(IdMaaS)

Nkosinathi Mpofu
School of Computing, UNISA
Science Campus, South Africa
mpofini@gmail.com

Wynand JC van Staden
School of Computing, UNISA
Science Campus, South Africa
wvs@wvs.za.net

***Abstract*— Identity management-as-a-service (IdMaaS) is a cloud computing service where the identity management function is moved to the cloud, streamlining the responsibilities of the computing or IT departments of organisations. IdMaaS's attractiveness leans on reduced cost of ownership, least to no capital investment, scalability, self-service, location independence and rapid deployment, however, its growth has been impeded by issues most of which are related to security, privacy and trust. Most organisations view identities as passports to key computing resources (hardware, software and data) as such they view identity management as a core IT function which must remain within the perimeter of sphere of control. This paper primarily aims to discuss IdMaaS and highlight the major trust issues in current existing cloud computing environments affecting the growth of IdMaaS by describing IdMaaS and surveying the trust issues that pose threats to its growth. Highlighting the trust issues hampering the growth of IdMaaS will lay a foundation for subsequent research efforts directed at addressing trust issues and therefore enhancing the growth of IdMaaS. Consequently the growth of IdMaaS will open up a new entrepreneurial avenue for service providers, at the same time enabling IdMaaS consumers to realise the benefits which come along with cloud computing. In future, we will analyse and evaluate the extent of impact posed by each trust issue to IdMaaS.**

Keywords - Cloud computing; identity management; trust; identity management-as- as-service.

I. INTRODUCTION

Internet services are fast expanding and continue to grow in response to customer needs, technological advancement and development. Such growth has given birth to a number of computing paradigms, one of which is cloud computing. Cloud computing in turn presented cloud opportunities like Infrastructure-as-a-service(IaaS), platform-as-a-Service(PaaS), Software-as-a-Service(SaaS), Identity-as-a-Service(IDaaS) derived from cloud service delivery models [1], and the still to mature Identity Management-as-a-Service (IdMaaS) among others. Key to the utilization of cloud services is mostly through identifying oneself, and the identity management function has matured to fulfil that role. A typical identity management system is composed of processes and technologies to manage and secure information and information resources of the organisation at the same time protecting user and customer profiles [2]. The basic elements of an identity management [3] regardless of who manages it include:

i. Directory – used to define and keep identity details of individual users
ii. Lifecycle management tools – used for adding , modifying and deleting of identity data from the directory system
iii. Regulatory mechanisms used to regulate user access to data. This may be achieved through policies or access privileges.
iv. Auditing and reporting tools – used to verify what has been happening to the systems, by whom and when.

In a traditional identity management system all four highlighted elements are within an organisation's boundary, whereas with the IdMaaS, the directory; lifecycle management and auditing and reporting tools will be hosted by the cloud identity management system provider.

Cloud computing is clearly one of the enticing technology areas partly due to its cost efficiency, scalability and flexibility. However, despite the surge in activity and interest, there are persistent concerns impeding its momentum. One such concern is trust which arises when the identity management function is ceded to a cloud third party. Lack of trust triggers an array of concerns like a) the fear that identities will be disclosed to undeserving parties b) identity security in storage, transit and during authentication c) mapping identities to services as well as d) provisioning and de-provisioning of services. Tackling trust issues will enhance the IdMaaS's appeal to cloud consumers thereby opening an entrepreneurial opportunity to cloud service providers, at the same time adding to the domain of anything-as-a-service(XaaS).

With many applications and systems migrating to the cloud, it may also be prudent to move identities closer to systems which utilize them. This will reduce the communication overhead and time required in transmitting identity information for purposes of authentication and service provisioning. IdMaaS utilizes a utility pricing model, as such, organisations can easily scale up or down to meet the changing needs, at the same time supporting mobile and geographically dispersed users at a much lower cost compared to identity systems managed locally. IdMaaS minimizes software management effort as this will be borne by the cloud identity providers. Above all IdMaaS enhances organisational focus by allowing organisations to focus on core business and not be side tracked by technology.

978-1-4799-3383-9/14/$31.00 ©2014 IEEE

The rest of this paper is structured as follows: Sections II provides a background of IdMaaS and trust, Section III surveys trust issues impediment to the adoption of IdMaaS and section IV proposes a framework which attempts to address trust issues surveyed in section III.

II. BACKGROUND

In this section we provide a background on IdMaaS and trust in order to establish the foundation for the issues with trust in cloud identity management.

A. *Identity Management-as-a-Service (IdMaaS)*

IdMaaS is a cloud service where a third party assumes the identity management role on behalf of identity owner (which is an organisation) leaving the organisations to devote almost their entire effort to the core business. IdMaaS increases staff augmentation, access to advanced security tools, access to contextual expertise, and positions information security and identity management as a business enabler [4], however its adoption diminishes owner's level of control over identities [5] triggering a risk of losing identity confidentiality, integrity and availability. IdMaaS is still to mature as a cloud service once issues related to trust are addressed. A typical IdMaaS environment at an abstract level consists of the identity provider (also acts as the identity manger in the cloud), identity owner (individuals, organisations or any other entity whose identity information is to be used for authentication purposes) and the relying party (website or online services which consumes identity provider services to obtain security credentials for users) as illustrated in Fig 1.

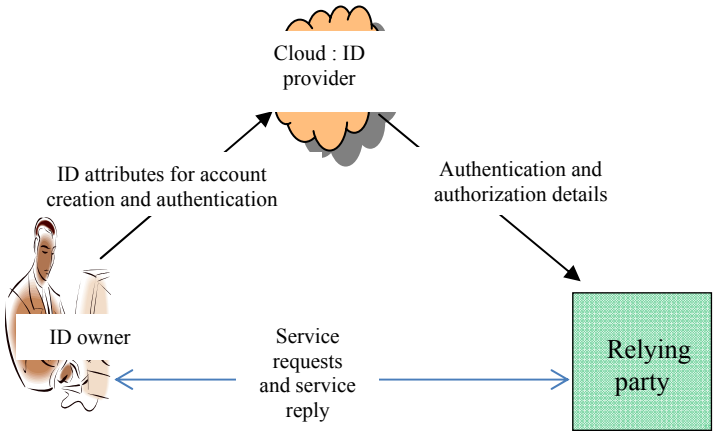

Figure 1. IdMaaS components

From Fig 1 above, the identity (ID) owner submits identity attributes for account creation or login details if they are existing users to the ID provider. The ID providers will do the authentication and transmits a package of authentication and authorisation details to the relying party. The relying party will respond directly to the users with the relevant services. Subsequent requests will now be directly to the relying party once a user has been authenticated. In case of account creation, the ID provider will create the account guided by the agreements they entered into with the relying party. In the eyes of the users it will seem as if they are authenticating directly with the relying party when in actual fact they are not.

Identity management systems are based on three trust models [6], namely pairwise, brokered and community trust models. The pairwise is used where two entities have a direct relationship with each other, whereas a brokered model [7] is related to the case of two entities that do not have a direct agreement with each other but have some agreements with one or more intermediaries so as to enable a business path to be constructed between them. The traditional identity management system is based on the pairwise model whereas the IdMaaS uses a brokered trust model whose trust issues are being surveyed by this paper.

B. *Trust*

Trust is an act of faith that relies on confidence that something will surely be delivered as promised [5] and can either be inherent or interpersonal [8]. The extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible [9] is also trust. Trust plays a vital role in the decision making process [10] and is built on prior knowledge and experience. The basic ingredients of trust is dependence, reliability and risk and terms such as confidence, belief, faith, certainty, assurance, reliance, sureness, credence have all been used in association with trust. Trust is non-transitive, asymmetric , biased towards personal opinion [11] , context dependent, subjective and evolutionary with time and new knowledge[10], making trust a very complex issue. There are some existing trust mechanisms trying to make the cloud as appealing as possible which includes service level agreements, policy based trust(public key infrastructure and certification authority) [12] , but have still fallen short of making the cloud a fully trusted platform.

III. SURVEY OF TRUST ISSUES

In this section we present the problems that exist with trust in identity management as a cloud service in order to elucidate the challenges that will have to be addressed. Trust is a necessity in situations where co-operation is part of the service provision structure. Trust is produced and Zucker [13] has identified the *institution*, *character* and *processes* as the major sources of trust. Trust issues manifests in the *cloud service* itself, the *service provider*, *cloud brokers*, *professional bodies* as well as the *legal system* [12]. Using two of the sources of trust as identified by [13] , this paper surveys trust issues from three trusting perspectives (Institutional, character and loss of control) as summarised in table 1 below

TABLE 1. TRUST ISSUES

Trusting Perspectives		
Institutional	***Character***	***Loss of Control***
• Competence • Interoperability • Confidentiality • dependability • Multi-tenancy • Auditability and accountability	• Fairness • Credibility • Predictability	• ownership and control over infrastructure • control over identity lifecycle • vendor lock-in • notification and redress • access and transparency

Table 1 provides a summary of trust issues categorised as either institutional, character or loss of control. Some of the issues overlap beyond a single category as discussed in the following sections**.**

A. Institutional based trust issues

Institutional-based trust [13] is tied to formal societal structures, depending on individual or firm-specific attributes. Institutional trust issues relate directly to the identity information, identity handling and the IT implicit in identity management. Issues of competence, interoperability, identity management system availability and multi-tenancy, are the prominent institutional issues as discussed in the following section.

- *Competence*

Competence issues are leaned towards the capability of the identity manager to handle and timeously respond to requests or calls which require the use of identities. Trust in competence according to [13] is based on the dynamic relationship between an individual (human or legal persona) and an institution (cloud ID provider/manager) participating in the identity ecosystem. The competence of the ID providers in managing identities on behalf of others is of paramount importance in the adoption of IdMaaS. Competence is dependent on knowledge and skill in protecting identity information, availing identities on demand, adapting to the ever evolving technological landscape, recovering from unexpected failures and to minimise identity management system downtime as far as possible. Consumers will always respond with reluctance in adopting IdMaaS if they doubt the competence level of the ID provider.

- *Interoperability issues*

IdMaaS is expected to be home to multiple identities belonging to multiple owners, as such there is a possibility of compatibility issues between the identity provider's system and the identity owners systems because of heterogeneity in platforms and approaches. Of the surveyed Chief information officers [14] 63% are concerned about integrating the internal and external services. Such a worry may be because of differences in platforms, protocols, software among others. A bid to make the systems homogenous calls for a compromise on either of the parties' party to the IdMaaS, a call some may be reluctant to heed. The ID provider's competence in making different systems interact is very necessary in allowing business continuity without making platforms homogenous. If the cloud service providers are not competent enough to integrate the different systems, then prospective consumers will respond with reluctance to the adoption of IdMaaS.

- *Dependability*

A dependable system is the most ideal as it naturally allows smooth transacting without fear of prejudice or any other form of a short change. Trust issues if not addressed affect the dependability of any system. "Dependability" is a system concept that integrates reliability, availability, safety, confidentiality and maintainability [15]. A dependable identity system is the one which is ready for service, continues to provide a correct service and able to undergo modifications and repairs in response to the changes in environment**.** To show the significance of dependability to trust, International Data Corporation (IDC) [13] found that 75% of the respondents were worried about cloud performance and availability, the key indicators of dependability. An ideal IdMaaS must be as dependable as possible if it is to be fully trusted and any deviations from the general principles of dependability will affect the adoption rate of IdMaaS.

- Confidentiality

Confidentiality is security in nature and relates to access to personal information in the identity management systems. The International Organisation for Standardisation (ISO) [16] defined confidentiality as "The property that information is not made available or disclosed to unauthorized individuals, entities or processes ". It is the expectation of the identity owners that their identities be protected from any exposure or abuse and if that is not evident, then consumers will naturally shy away from IdMaaS. The basic competence of the ID provider is measured by their ability to guard identities against unauthorised access or disclosure, destruction (accidental or unlawful destruction or loss), modification and unauthorised use[17]. Any organization which fails to show its competence in preserving confidentiality is likely to prolong one's stay off-the cloud.

- *Multi-tenancy issues*

Multi-tenancy issues arise when a multi-tenancy model is being utilised as a deployment model. Multi-tenancy allows a single cloud instance to be used by different consumers resulting in data(identities) for the same instance being stored on the same database[18]. This may result in identity or data leaks across users of the same instance resulting in loss of confidentiality and an increased exposure to other hostile tenants. Also sharing a cloud with tenants who are strangers reduces the trust consumers place on the cloud service. Policies stating the behaviour of the cloud participant coupled with defined minimum security provisions (by Id provider) may come in handy in addressing the multi tenancy problem

- Auditability and accountability issues

Accountability and auditability is all about knowing what is happening, and holding individuals or other entities accountable for their actions or that of their agents. One major activity of accountability and auditability of cloud providers is the tracking of file access history. This will help in knowing what happened to the file, when and by whom. Any increase in accountability and auditability activities will help address five of the top 10 security risks as identified by Cloud Security Alliance [19] and corroborated by [20], and these are:

i. Abuse and nefarious use of cloud computing
ii. Insecure application programming interfaces
iii. Malicious insiders
iv. Data loss or leakages
v. Unknown risk profile.

To simplify accountability and auditability, [20] have identified three abstract layers to be targeted for accountability

process and these and these are system layer(operating system, file system and network logs), data layer as well as the workflow layer. The system layer tracks the lifecycle of the file whereas the data layer focusses on the lifecycle of data while the workflow layer is more focussed on governance and business process issues. Accountability is a basic ingredient of trust and once there is no accountability and auditability, mistrust in the service are inevitable making consumers to shy away from adopting cloud services.

B. Character trust issues

Character trust issues relates to the behaviour of the cloud identity provider. The character of a cloud participant helps others to predict their behaviour. Fairness, credibility, dependability are some of the characters which may either enhance or diminish one's trust on the cloud participant.

- *Fairness*

Trust and confidence in the IdMaaS are related to whether the ID provider is seen as being fair in the eyes of the identity owner and the relying party. One party to the IdMaaS ecosystem will be more likely to trust the other if it believes that it will not be unfairly taken advantage of. Fair practices were developed by the US in 1970s [21]and later adopted and declared as principles by the Organisation for economic and Development(OECD) [22], of which some have been adapted to come up with fair practices principles for IdMaaS. The fair practices principles as applied to identity management state that identities should:

i. be collected legally and with the consent of the data subject
ii. be relevant and kept up to date
iii. not be used for other purposes
iv. be protected by a reasonable degree of security
v. specify other uses of identities held by the cloud identity service provider

Violation of the fairness principles diminishes the level of trust cloud service consumers place on IdMaaS.

- *Credibility*

Renn and Levine in[13] argue that trust and confidence in an organisation or institution is directly related to their credibility. Credibility is based on past relationship, encounters as well as how peers perceive an institution. Graig [23] identified eight principles which can be used to gauge the level of credibility one can place to the identity service provider, and these are:

i. The actions of the cloud identity service provider should always be in tandem to what they say. If there is a disparity between what is said and what is done then the credibility gap widens.
ii. Cloud service provider should always talk to the cloud consumers and face to face is the best medium.
iii. Cloud service providers should ensure full disclosure of their offering to the cloud consumer.
iv. Cloud service providers should be tolerant to employees who speak up the truth. Fear of retribution for speaking up the truth sends a negative signal to the consumers on the genuineness of the cloud ID provider.
v. Service provider should always accept feedback from the consumers as this will help in improving the service.
vi. The structure of communique between the service provider and the consumer should be simple and clear.
vii. Communication should always be on time every time.
viii. Cloud service provider should always find a way of getting the job done than giving

Trust in IdMaaS will be enhanced if the credibility gap is narrowed by upholding the principles of credibility.

- *Predictability*

Predictability is defined in the Cambridge dictionary as "the state of knowing what something is like, when something will happen". Predictability is based on consistency in past actions and is relative to the relationship between two or more entities. A Cloud identity service provider must deliver a service in a manner that assures a consistent experience to the cloud consumers in order to achieve predictability. This predictability may be achieved through the homogenization of underlying service provision system (physical servers, network devices, and storage systems). Predictability may be driven through the standardization of service as well as processes from the service management's point of view. Predictability as a principle is necessary in driving service quality, and once quality service has been achieved, the attractiveness of IdMaaS will be difficult to resist. Predictability leads to a stable and flexible relationship between the cloud service provider and the cloud identity system consumer.

C. Loss of control issues

The adoption of IdMaaS requires a huge concession on the control over identities by the identity owners. The key aspects affected by lack of control and needing attention as identified in [17] includes ownership and control over infrastructure and identity lifecycle; vendor lock-ins; and transparency as discussed below :

- *Ownership and control over infrastructure*

Control over the underlying infrastructure hosting and the identity lifecycle is solely in the hands of the service providers. Service consumers will most likely feel uneasy especially if they are unsure on how secure the infrastructure is. This then calls for transparency on hoe the cloud identity system is secured. This uneasiness affects one's faith in IdMaaS and will respond to the uptake of IdMaaS with reluctance.

- *Control over identity life cycle issues*

Identities go through a number of stages throughout their lifetime as such the actions of the identity manager on the identities at different stages of the identities must not be in doubt. The identity owners will need to trust that actions requested on identities are executed as requested, however that can only be possible if there is a clear inclusion to that effect in

contractual agreements made. For example in case of a requested deletion of an identity(s) it needs to be clear that the action has been executed and who retains the identities, for how long. The absence of procedures and policies to guaranteeing performance and outlining what happens to the identities in their lifetime is a policy issue making the cloud un-attractive.

- *Vendor Lock-in issues*

IdMaaS is still in its infancy, as such, the probability that the identity system provider may not be compatible with cloud consumer's systems is significant. This will make cloud system consumers to adopt a wait-and-see approach as they feel early adoption may result in vendor lock-ins. The gravity of vendor lock-in as an issue is highlighted in the research by IDC [14] who found out that 79% of the Chief information officers who participated in the survey are reluctant to go for fear of being tied to a single vendor. This fear may be curtailed by developing standards to allow for interoperability of identity management systems from different vendors to allow for simple vendor changeover without seriously reconfiguring the system.

- *Notification and redress*

In case either party within the IdMaaS ecosystem is aggrieved, there should be some formal procedures to seek redress. However, where control has been lost or reduced, it becomes difficult to know of the occurrence of privacy breaches and the individual/organisation at fault. The absences of mechanisms for notification or for redress in case of breaches reduce the attractiveness of the cloud identity service.

- *Access and transparency*

Naturally, cloud identity systems consumers will always want to know where their identities are, who owns them and what is being done with them. A transparent identity management provider opens up its inner workings and provides access to timely information to other stakeholders so they can make informed decisions and choices as well as to hold the cloud identity provider to account for their actions, goals and objectives. Increased transparency improves stability and fosters the development of a sustainable identity management system as it also provides for stakeholder input towards making the cloud as habitable as possible. Lack of processes which promote easy access to information and transparency becomes an issue limiting the trust one can place to the IdMaaS.

IV. ADDRESSING TRUST ISSUES

In light of the trust issues discussed, the basic roles and relationships of IdMaaS participants, implementation mechanisms and the type of exchange relationships will need to be well defined. A trust framework will come in handy in providing a set of technical, operational, legal requirements and mechanisms for exchanging identity information and data. The framework will thus provide:

i. IdMaaS roles and relationships – This section will specify the relationships and roles of the:
   - policy makers
   - IdMaaS providers;
   - assessors who evaluate the identity service provider and certify their capability
   - auditors who check if the party's actions conform to agreements
   - dispute resolvers who arbitrate in case of a misunderstanding between IdMaaS parties
   - Cloud consumers who utilise the cloud identity service.

ii. Implementation mechanism – This sets down mechanisms for implementation and includes the criteria for measuring the cloud identity service provider's capability as well as the certification process.

iii. Legally binding agreements – The strength of the framework will be based on well-formed agreements which include:
   - identity service provider certification agreements
   - assessor agreements,
   - terms of service agreements
   - Memorandum of agreements.

The proposed framework is generic and adaptable to meet specific industry needs without violating the basic principles of privacy, flexibility, voluntary participation and trust.

V. CONCLUSION

Investing in building and maintaining a trusted service is a basic requirement to the success of any cloud service. Processes which define the procedures and guidelines for one's participation in the cloud are a first step in establishing a trusted cloud identity service as it simplifies cloud governance. Processes provide guiding principles for controlling behaviour after loss of control, mechanisms for accountability and auditability and promote co-existence, making the cloud the most habitable computing paradigm. A trusted service is likely to have fewer complaints arising; as such the character of the cloud service provider has much bearing on the attractiveness of IdMaaS. Providers who are transparent and inclusive of all stakeholders in decision making are likely attract most cloud consumers.

Trust is a complex phenomenon that can derive from different sources and take multiple forms. Trust affects the perceptions about IdMaaS and influences decisions related to the uptake of IdMaaS, as such, trust becomes a precondition to the success of IdMaaS. Trust issues can either be Institutional, character or loss of control and addressing them offer an integrative potential amongst the IdMaaS ecosystem's participants. A trust framework is one way of enhancing the attractiveness of the concept of IdMaaS, and with the identified trust issues, there is now a foundation on which to formulate a trust framework for IdMaaS as our next research focus.

A further research may be necessary to establish the impact of each the issue towards the overall trust level one can place on a cloud identity service. The weighting of each trust issue will be an invaluable input to the refinement of the proposed trust framework.

REFERENCES

[1] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1–11, 2011.

[2] P. Wood, "Implementing identity management security - An ethical hacker's view," Journal of Network Security, vol. 2005, no. 9, pp. 12–15, 2005.

[3] J. Walters, "The ABCs of identity Management," 2004. [Online]. Available: http://www.csoonline.com/article/205053/the-abcs-of-identity-management. [Accessed: 16-May-2013].

[4] J. Graaneman, "Security as a Service : Benefits and Risks of Cloud-Based Security." pp. 2–10, 2011.

[5] K. M. Khan and Q. Malluhi, "Establishing Trust in Cloud Computing," IEEE Computer Society, no. October, pp. 20–26, Oct-2010.

[6] S. Boeyen, G. Ellison, N. Karhuluoma, W. Schlumberger, P. Madsen, and S. Sengodan, "Trust models Guidelines." OASIS.

[7] A. Bhargav-spantzel, A. C. Squicciarini, and E. Bertino, "Integrating Federated Digital Identity Management and Trust Negotiation – issues and solutions," pp. 1–15.

[8] R. Sampath and D. Goel, "RATING: rigorous assessment of trust in identity management," in First International Conference on Availability Reliability and Security ARES06, 2006, p. 10.

[9] D. H. Mcknight and N. L. Chervany, "The meanings of trust," Measurement, vol. 55455, no. 612, p. 86, 1996.

[10] M. Firdhous, O. Ghazali, and S. Hassan, "Trust Management in Cloud Computing : A Critical Review," International Journal on Advances in ICT for Emerging Regions., vol. 04, no. 02, pp. 24–36, 2011.

[11] K. S. Ramana, "A Survey on Trust Management for Mobile Ad Hoc Networks," International journal of Network Security, vol. 2, no. 2, pp. 75–85, 2010.

[12] J. Huang and D. M. Nicol, "Trust mechanisms for cloud computing," Journal of Cloud Computing: Advances, Systems and Applications, vol. 2, no. 1, p. 9, 2013.

[13] L. G. Zucker, "Production of Trust: Institutional Sources of Economic Structure, 1840-1920," Research in Organizational Behaviour, vol. 8, pp. 53–111, 1986.

[14] IDC, "IDC Enterprise Panel, SEPTEMBER. http://www.slideshare.net/JorFigOr/cloud-computing-2010-an-idcupdate," 2009.

[15] Jean-Claude Laprie, Dependability — Its Attributes, Impairments and Means. Springer Berlin Heidelberg, 1995, pp. 3–18.

[16] ISO, "ISO 27001: Information Security Management – Specification With Guidance for Use." 2005.

[17] S. Pearson, "Privacy , Security and Trust in Cloud Computing Privacy , Security and Trust in Cloud Computing." Springer Berlin Heidelberg, 2012.

[18] K. Hashizume, D. Rosado, E. Fernández-Medina, and E. Fernandez, "An analysis of security issues for cloud computing," Journal of Internet Services and Applications, vol. 4, no. 5, pp. 1–13, 2013.

[19] Cloud Security Alliance, "Identity and Access Management in the Cloud." pp. 3–19, 2010.

[20] R. K. L. Ko, B. S. Lee, and S. Pearson, "Towards Achieving Accountability , Auditability and Trust in Cloud Computing," Scenario, vol. 193, pp. 432–444, 2011.

[21] "Personal Privacy in an Information Society, United Statues Privacy Protection Study Commission Fair Information Practices." Privacy Protection Study Commission, 1977.

[22] OECD, "Guidelines for the Protection of Personal Data and Transborder Data Flows." Organization for Economic Co-operation and Development (OECD), 1980.

[23] G. Borosowich, "Walk the talk - 8 Principles of credibility," 2006. [Online]. Available: http://it.toolbox.com/blogs/enterprise-solutions/walk-the-talk-8-principles-of-credibility-12095. [Accessed: 18-Apr-2014].