TRUST IDENTITY MANAGEMENT MODEL (TIDM): A HEURISTIC APPROACH

Peter Okpamen*

Abstract:

The issue of "Trust and Identity Management (TIDM)" refers to the analysis of procedures of utilizing technologies, models/methods, standards/mechanisms in order to manage essential information in the corporation network about the identity of every entity users and control access to business resources. The study centres on TIDM solution analysis and defines how Identity Management (IDM) domain can achieve its objectives to get a better productivity, security, and efficiency of Digital Identity based communication in line with business operation and transaction while minimizing costs related. This study will also involve an extensive view of how effective and reliable the TIDM obtains its objectives such as letting enterprises to acquire secure Network access and admission, while isolating and controlling infected devices that may attempt to access the Network. Similarly, the study also analyse and emphasize how TIDM guarantees the Identity and Integrity of every entity on the Network in order to apply appropriate access policy, deliver visibility into Network activity, and secure the local, centralized, distributed, federated, and web/globalizes management of remote devices, while providing Authentication, Authorization, and Accounting functionality across all Network devices.

* PhD

1.1 INTRODUCTION

This research is set out to analyse workability, and benefits of administration of personal digital Identity-attributes in a given environment; as well as to address issues, solution, and scientific approach in solving issues of Identity Management (IDM). Benantar (2006: 40-53) portray IDM as not only providing capability of management of digital identities in locally and centrally managed environment; but also providing the key requirements such as the secure and efficient administration of numerous digital identity attributes of each individual in distributed, cross-domain and even in Internet level/Web IDM.)

IDM has suddenly become the source of creating Internet based business and it provide benefits such as cost saving, administration control, efficiency in operation, and growth of business.
Successful operation of any ID management in enterprise/business is based on secure access to various relevant information and applications scattered all over computer systems situated both in the internal and external world of the enterprise. In addition, such information and application provides access to the increasing number of users; both in and out of the enterprise without compromising sensitive identity information. Issues of Identities data privacy compliance are also likely to take place as IDM can even be used to manage multiple accounts of users' identities across numerous inheritance applications that make the IDM task even menacing and scary (Shim, Bhalla, & Pendyala, (2005).

However, IDM processes are not complete process by themselves. They need to be supported by a strong foundation of trust. Most importantly, the trust plays a vital role, while establishing Identity in cross-organization environment in order to provide control over the identity entitlements. In particular, the basic goal of this research is to have an in-depth study of a related Case Study to ascertain the viability of Trust and Identity Management system and mechanism. This however is the first in three series of this research work. The second series shall encompass discussion on Federated Identity Management Mode; while the last of the series shall deal on the implementation of Electronic IDM Network of federation of "GP-Patient:"—Towards Preventing Identity Conflicts in NHS.

1.2 OBJECTIVE OF THE STUDY

The basic objective of this project is to provide an in-depth understanding on the usefulness and limitation of Trust and Identity Management (TIDM); and identify ways to achieving Identity Management (IDM) in an existing scenario through a comprehensive description, and analysis of an IDM model.

1.3 RESEARCH QUESTIONS

In view of the fact that most organizations are interested in managing the identity of its clients, employees; as well as its resources of Network; this research will therefore lead us into some basic questions listed below:

- What is Identity and Trust?
- What are Identity Management and Trust Management?
- What are types of models of IDM, their workability, benefits and limitations?
- Why is it important to address Trust and Identity Management system in organizations?
- How Trust is measured in Identity Management?
- How Trust and Identity Management controls Network access?
- What are the methods of Trust and Identity Management?
- What are the types of Trust used in Identity Management?
- What are the standards/mechanisms of Identity Management?

1.4 STATEMENT OF THE PROBLEM

- Providing secure and efficient management of Identity has been a challenge to many corporate users, and the need to break the barriers initiating against its efficiency is vital for this research.
- It is also a challenge providing distributed Identity information over the Internet as against making convenient by registering ID and password and using it in many websites.
- Handling Identity base e-businesses is also a complex task as they have to cope with the enormous demand of providing services to various entities.
- Due to fast evolution of Identity there seems to be lack of time to adopt proper Identity handling to the new environment such as legislation, society, and economy.

- Since Identity handling is deeply concerned about sensitivity of security and privacy, it seems that IT environment is saturated with continuous changes; such as mergers and acquisitions, supply chain activity, staff and client turnover, and authoritarian differences.

1.5 SIGNIFICANCE OF THE STUDY

- It will enable the reader or user to understand and find out how Identity Management provides greater opportunity beyond the process of authentication and authorization of users.
- It will provide knowledge to system developer, managers and other users on how the online services of an organization are managed from internal perspective and customer self care perception.
- It will also provide information as to what system infrastructure components are required that basically deliver services to users when they demand using particular Network technology.

Literature Review

2.0 The Concept of Identity Management (IDM

2.1 WHAT IS IDENTITY?

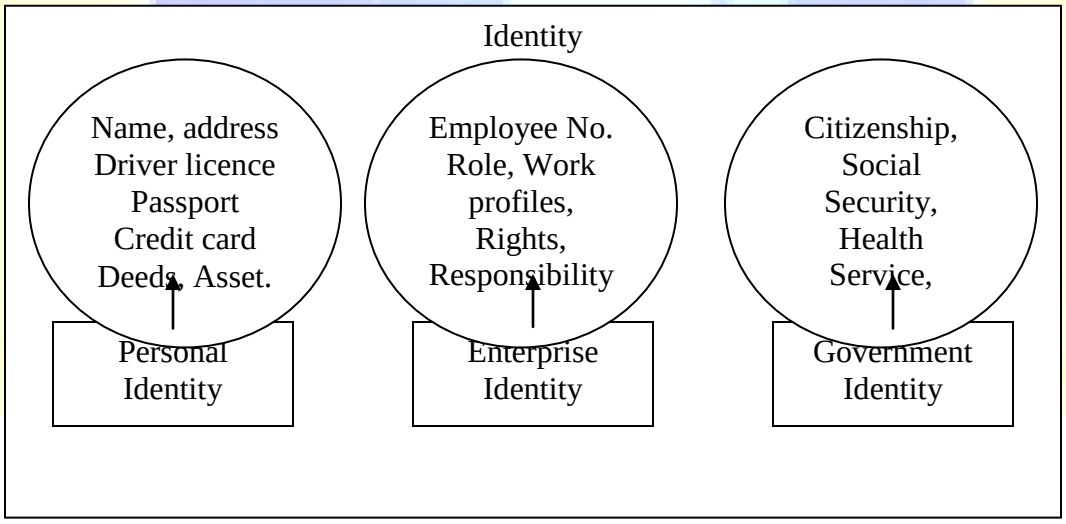

Figure 1 Example of Identity and its profile

Source: Researcher's work

Corrandini et al (2006), describe identity as a source of information of any individual, such as human being. Such information represents the particular individual digitally to be recognized as who he/she claims to be. It implies that Identity refers to a subset of an entity e.g., name, address, credit card, Passport etc; while digital identity is capable of recreating, organizing, automating and integrating the aspects of Identity in the electronic world.

2.2 WHAT IS IDENTITY MANAGEMENT?

Essentially, Identity Management (IDM) is simply a management of attributes of user identity and their accesses in the Network and online system environment. This means that the good management of user credentials also refers to as identity attribute profiles is responsible for claims verification made by identity to prove who he/she is so that they can access resources.

Hatala et al (2007) maintained that identity must be dealt by providing adequate security constructs like authentication that can verify the claims. However, the security construct part of IDM includes an in-depth discussion of authentication and access control. Thompson, R.D & Thompson. C, (2007), maintained that IDM can help the individual to gain recognition according to the requirement of a given environment. Benantar (2006: 40) views IDM as dealing with a wide administrative area, in which it deals with individuals Identity attribute profile in order to identify them in a network etc and control their access to resources. Cunningham (2004) states that '… Identity is specified as all information associated with an individual (not only digital certificates). He further opined that there are many other approaches in relation to defining IDM. However, in line with this, according to Herreweghen and his team as quoted by Cunningham (2004) in his book titled "adoption and the Knowledge Economy Issues, Applications, Case Studies" Page 848, 'IDM is a part of an end-to-end security solution and addresses the needs for certainty in the areas of authentication, access control and user management.

In today's Internet World, internet access has provided more ways of opportunities for enterprises, government, people, including the availability of Web services and means of communication in relation to providing as much online services as possible on demand, and it has also led to deploying infrastructures in order to make electronic businesses and interaction possible. This means that in this emerging e-world, IDM is all about fulfilling the needs of different e-players such as e-businesses and e-commerce by identifying entities in order to

advance trust and respect for information security, privacy, and data protection. IDM is about enabling business organizations to enlarge the scope of the services they offer. This implies that IDM can facilitate businesses to computerize and expand enormous business processes and transactions, while enabling to support the principle of collaborative commerce by way of implementation of several Digital Identities that enabled Internet users to face various corporate applications and e-business interfaces as IDM solution controls complexity of such environment.

Fuchs and Pernul (2007), views IDM 'as a subset of attributes or characteristics of an entity which makes the entity, e. g. a person uniquely identifiable within a set of entities'. It implies that even an entity is recognised as itself, but can be associated with multiple electronically representing identities that enable it to work with different applications. In IDM, each identity is enforced and managed to be associated with unique access information and the information is managed by creating it, maintaining it and erasing it separately.

2.2.1 ENVIRONMENT OF IDENTITY MANAGEMENT

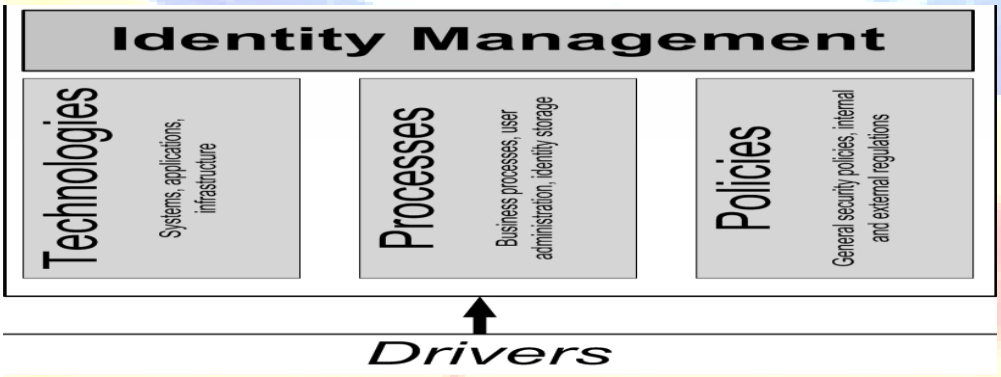

Figure 2 Environment of IDM

Source:

http://0ieeexplore.ieee.org.lispac.lsbu.ac.uk/iel5/4159773/4159774/04159826.pdf?tp=&arnumber=4159826&isnumber=4159774.

The above figure 2 describes a typical IDM environment that consists of an integrated framework of well defined 'Processes', 'Policies' and 'Technologies'. These aspects however,

function under the guidance of organizational and technical driver that deals with the lifecycle of Identities e. g. storage, allocation and revocation of user resources (Fuchs & Pernul, 2007).

2.2.2 ASPECTS OF IDM IN ORGANIZATION

The IDM aspects in organization are based upon its environment as defined above. Defining processes and policies of IDM creates the foundation for a subsequent implementation of IDM by regulating the usability of electronic identities. Defined policies and processes in the organizational environment make technological measures useful as processes deals with user management, technical and organizational approval of workflows and escalation procedures. Policies then help to regulate Identity related information flows by defining, consolidating and harmonising on different levels in the organization e.g. process level, IDM-level, IT or global level (Fuchs & Pernul, 2007).

2.2.3 IDM DRIVERS

The figure 2 of IDM environment makes us to understand that the driver influences the way IDM environment framework acts. For example; technological aspects set its goal by defining security, scalability, system performance and process automation, while management aspects is guided to create overall strong security, less investment or cost in administration and more efficient processes of user management and control (Fuchs & Pernul, 2007).

2.2.4 TECHNOLOGY IN IDM

Due to users' Identity profile and sub-systems profile management IDM is no longer easy to perform within confined scope of single functional components. Organizations need comprehensive, integrative and standard-based IDM infrastructure that contains several functional model of IDM environment each serving different purpose.

However, due to greater need for exchange of identity data to communicate securely beyond single-domain there is greater need to create standardized data exchange channel. In order to fulfil this obligation, the State of the-art identity federation must rely on open standards, such as

the XML-based protocols SAML', or SPML. Below is a figure illustrating the technological aspects of IDM.

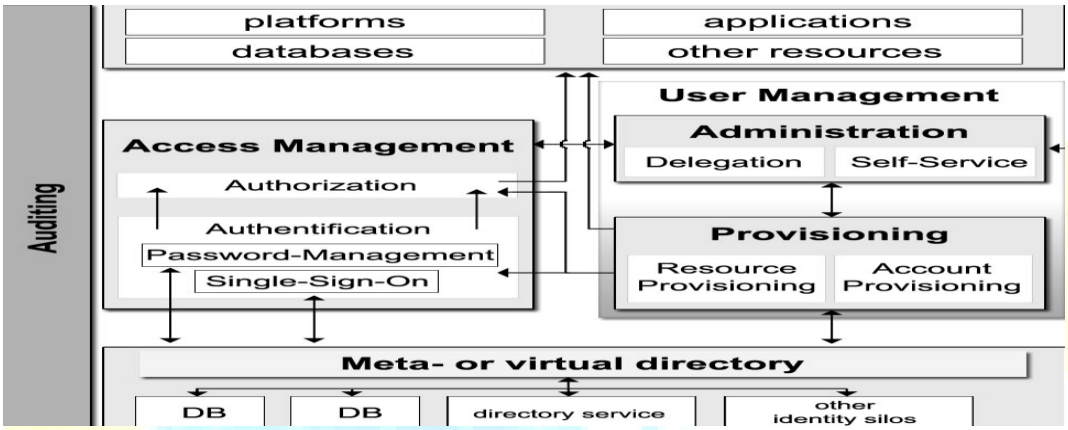

Figure 3 Example of IDM infrastructure of local IDM environment:

Source:

http://0ieeexplore.ieee.org.lispac.lsbu.ac.uk/iel5/4159773/4159774/04159826.pdf?tp=&arnumber=4159826&isnumber=4159774.

Figure 3 above encompass technologies involved in IDM within an enterprise. Generally, IDM technological aspects consists of 'Directory services, User management, and Access Management' as technological models in IDM.

2.2.5 DIRECTORY SERVICES AND USER MANAGEMENT

Directory service provides IDM services by enabling users and resources information to be synchronised, while forming the fundament of a comprehensive IDM infrastructure. User management provide services to IDM by facilitating data provided by directory services and managing the digital identities throughout their lifecycle. Basically, it creates and terminates user account. For example; when an employee leaves an organization, user management is de-activated by de-provisioning the Identity status and it function in such a way as to make sure the rights of inactive users are locked, revoked as quickly as possible in order to control security.

2.2.6 ACCESS MANAGEMENT

This is also one of important aspects of IDM infrastructure that deals with users' authentication and authorization in relation to connecting to resources. According to Butler Group (2006: 51) access management enables the right user to get defined access on the basis of his/her defined and managed role rather than on individual IDS. It also includes Single Sign on (SSO) and other methods of authentication e. g. Password, digital certificate and hardware and software tokens. For the purpose of this study, access management will not be discussed beyond this point; rather emphasis will be centred on Trust and Identity Management.

2.3 WHAT IS TRUST?

Even though there is no specific definition of trust, a school of thought defines trust as: "assured reliance on the character, ability, strength, or truth of someone or something". They also define trust as the "firm reliance on the integrity, ability, or character of a person or thing". Organizations therefore, may share data with one another across what is called a global info-sphere that spans multiple info-spheres'. In order words, there is a critical need for organization to share data across single and multiple domains of organizations and internet at global level.

While there is need to exchange sensitive data across multi domain environment, there is also concern coming up, such as Cyber-crime and threats to national security that costs billions of dollar in the world. It is this Trust that enables Identity establishment, which enables an entity to be competent, consistent, and dependable in the process of authentication.

However, Trust fulfils greater need to exchange data while fulfilling the process of sharing data within and across boundaries of organizations. Nevertheless, there is a greater need to secure Identity information while sharing within, cross-domain and global level. Trust management however, do face a lot of challenges; for instance, to enforce the right management procedure as well as security policies while exchanging data in various environments.

2.4 WHAT IS TRUST MANAGEMENT?

According to Thuraisingham (2005) Trust refers to that factor that makes us to believe on a second person to implement policies that have been created, regulated, and enforced on data information. In other words, an entity X can trust another entity Y, but X may not necessarily trust a third entity Z. However, in such condition, the entity X provides information to the entity Y believing that Y will not provide the information to the third entity Z. There are mechanisms available in order to support trust establishment that will offer trust services such as 'Identity Services', 'Authorization Services' and 'Reputation services'.

The concept of Trust is also used in different fields but in the field of Network computing environment, Trust is all about defining descriptions of different entities so that the defined descriptions can be supported by Trust concept to facilitate Trust relationship between entities, and enable the system to exchange information smoothly.

This means that Trust Management systems in line with Identity Management in networked computing environment is all about how to provide access to resources and information, depending upon trustworthiness of users, while using Trust as a measure of resources and information to be allowed to access. Trust Management also promote decisions on whom to trust and to what degree, while facilitating interaction in pervasive computing environment.

In view of this development, it is evident that Trust and Identity Management (TIDM) is related to each other via process of establishing trust and secure relationship based upon claims made by one party and validating the same by other trusted parties in order to engage those parties in commercial and other interactive activities (http://blogs.sun.com/identity/entry/identity_management_or_trust, 2007).

Besides Identity Management system model, the Trust Management model built is concerned with creating Trust based on institutionalised trust in the environment of offline world; and Trust made on the basis of analysis of record of experience from the online world. Trust Management is all about enabling an individual or organization already existing with Trust relationship in the offline world environment to connect and assign values of Trust and issue certificates to involved entities in the online world in order to generate a network of Trust for users on top of Peer-to-Peer systems, which then makes users able to interact with unknown entities or peers in the

system asking about others opinion before any transaction takes place (http://www.create-net.org/osco/publications/ion-tele-bott-kosh-eBusiness-07.pdf.

Similarly, in relation to Trust Management, Benanatar (2006: 73) states that *'**T**he entity performing authentication is presented with information that only the entity being authenticated is able to provide'*. The idea behind this is to explain that Trust Management is concerned about how an authenticating entity establishes a guarantee or assurance "Trust" performing authentication in such a way that an entity asserting for authentication along with a particular Identity, needs to declare its claim by supplying verifiable and provable information as a proof of possession (POP) of Identity to the authenticating entity in order to set up Trust through a process of secure confirmation and verification.

2.5 CONCEPT OF TIDM MODEL

This aspect contains a discussion on the various methods/models and protocols associated to Trust and Identity Management. Essentially, the system links and its function of different IDM methods/models will be included in this discussion. The core product of the discussion shall be the issue of central trust involved in the management of Identity. Each concept on TIDM methods/models is followed with a brief highlight of its benefits and limitations. Below are some methods/models of IDM and associated Trust method:

2.5.1 LOCAL IDENTITY MANAGEMENT MODEL

Local IDM is about managing each application individually where as not collectively using directory service as the central point of multiple applications. The idea behind Local IDM is that, it is a host system that keeps and run a local registry of all users' identities to be locally known to the system. Any user who may wish to use the system for purpose of authentication to access resources from the host computer or system domain needs to acquire an Identity in order to be able to use the resources. The figure below is an illustration of Local IDM.

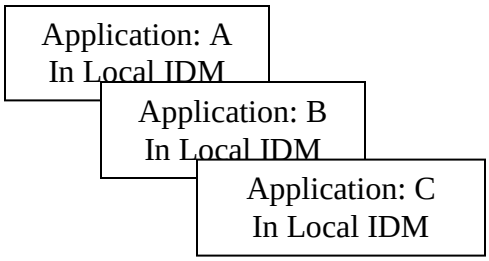

Figure 4 Example of Local IDM network

Source: Stefan (2004) pp195:

Benanatar (2006: 41), is of the view that user management in Local IDM is done by registering Identity information first in the local host system domain in order to use Identity information as reference when an entity request for identity establishment and authentication. It implies that any addition of Identity must be unique from pre-defined one in order to facilitate addition and removal of Identities without affecting other Identities as each application becomes individual operation. This also means that each managed entity is associated to his/her privilege that may have been defined over the local system resources. The figure below is an example of Local IDM.

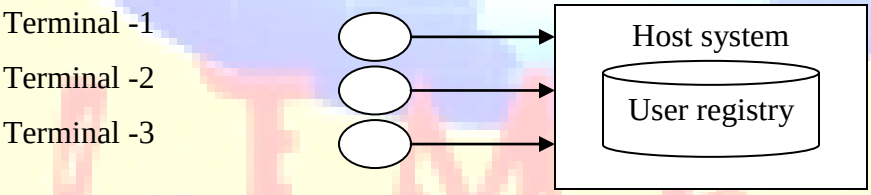

Figure 5 Example of Local IDM network

Source: Messaoud (2006: pp42)

The figures above, 4 and 5 are examples of Local IDM network based on the concept of Local IDM. In particular, user management is carried out by implementing Lightweight Directory Access Protocol (LDAP) based on X.500 ISO standard. Single Sign-on (SSO) is used for Identity authentication and directory services and is accessed via TCP/IP. Figures 4 and 5 above refer to systems on Local IDM network e. g. Application: A to C and Terminals: 1 to 3 needs to maintain separate user registry access in Local host system.

2.5.2 TRUST IN LOCAL IDM MODEL

According to Benantar (2006: 74), Trust in Local IDM is built under shared secret. For instance password, this is required to be unlike for every system to be accessible for that user. Identities in Local IDM are recognized only within the defined local scope and range, while in such environment, Identity trust is established through ***bipartite trust method***. It describes trust in a graph mapping containing a column of users represented by (X) and column of installed systems represented by (Y). As a result, such tie between entities like (X) and (Y) creates Trust relationship between the entities formed on the basis of shared secret relationship. Below is a figure expressing a Bipartite Trust method in Local IDM.

Graph (G):

Users' column (X):

Edge or links (L):

Systems' column (Y):

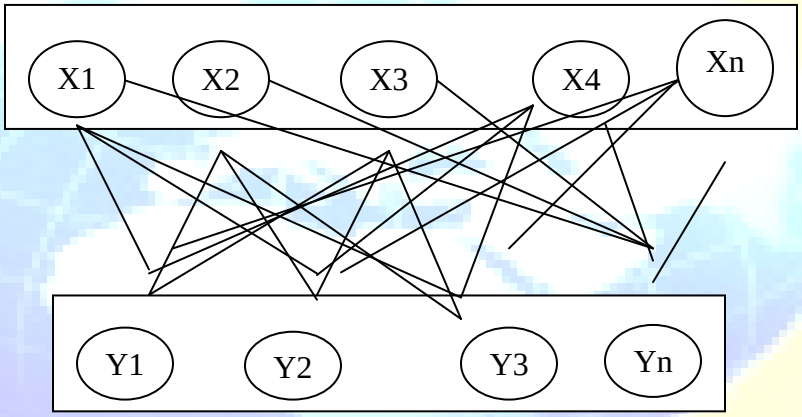

Figure: 6 Bipartite Trust methods in Local IDM.

Source: Messaoud (2006) pg 75:

The figure above represents an example of bipartite Trust Management method at Local IDM in which column (X) contains various users and column (Y) contains installed systems. The figure represents a graph mapping that contains (X) users and (Y) systems creates (X×Y) relation that binds all entities together, creating and managing secret sharing relationship in order to create Trust for authentication among all entities in Local Identity Management.

The above graph contains two disjoint sets nodes e. g. users denoted by (X), systems denoted by (Y), graph denoted by (G) and links denoted by (L). X and Y are like two sets whose relationship

is disjointed. As the provision of establishing trust in Local IDM is based on sharing secret between each entity, on the basis of graph (G) forms the relationship between entities by links denoted by (L) that can be expressed as following.

Quantitatively:

G = (X × Y, L), where

L = Symbol of links connecting variables X and Y;

X = (x1 + x2 + x3 + …… xn); and

Y = (y1 + y2 + y3 + …….yn).

These equations forms the relationship based on secret sharing; e. g. password; as two vertices or nodes (X and Y) in graph (G) are connected by defined path or links (L) X to Y and Y to X of each other that enables it to establish trust in order to gain access for services. The relationship of trust is as follow.

G = (X × Y)

G = {(x1 + x2 + x3 + ……xn) × (y1 + y2 + y3 + ……yn)}

2.5.3 LIMITATIONS AND BENEFITS OF LOCAL IDM MODEL

Benefits:	**Limitations:**
Locally visible, simple to manage. Flat-name-scope controls scope of identity by resulting in name collision against any duplication. Addition and removal of identities without effecting others and identity synchronization is easy within local host system. (Benantar, 2006: 74)	Identity scope is confined within local host only that does not allow cross-domain communication for identification. Identity scaling capacity gets affected as number of users and subsystems are increased and data scalability problem occurs due to defined confinement. (Benantar, 2006: 74)

Table 1: Local IDM model benefits and limitations

2.6 CENTRALIZED IDENTITY MANAGEMENT MODE

Centralized IDM is about making IDM simple, by managing the process of access-control from several individual applications to a single centralized authority, a directory. In this case 'User management is no longer a separate issue from each application individually'. Below is an example.

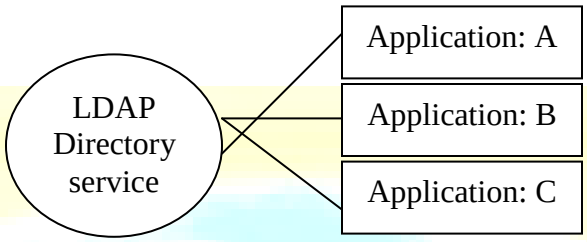

Figure 7 Centralized IDM network

Source: Stefan (2004) pg 195:

Broadly speaking, Centralized IDM helps to avoid the issue of maintaining access-control to each registered application that exists in Local IDM. Benantar (2006: 67) maintained that 'It enables a single view of the multitude of systems in the enterprise and provides a consistent interface to all the systems; as well as unifies identity-management processes'. In other words, implementation of the model enables large organization to control cost in management aspects and guarantees IDM elements to be controlled within the organization's local domain. Below is a sample description of Centralized ID:

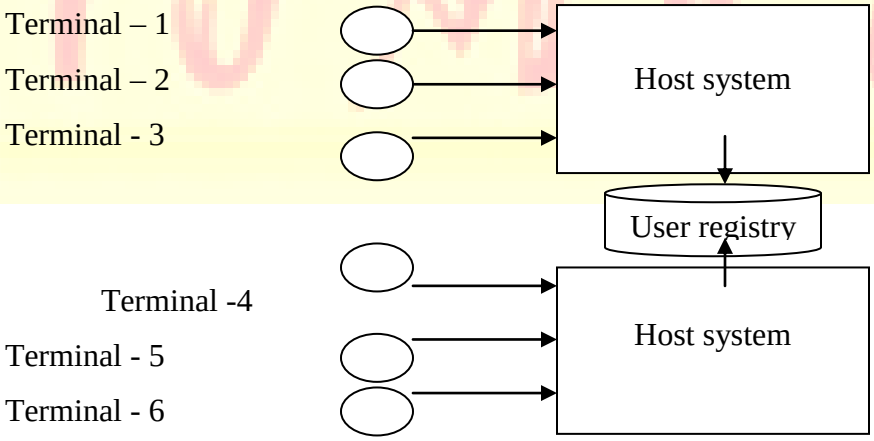

Figure 8 Centralized IDM network

Source: Messaoud (2006) pg 42:

The figures above are the examples of Centralized IDM which indicates that the user registry is joint and mutual to share with several systems; e. g. Application: A to C and Terminals 1 to 6 respectively. That means, Central IDM model allows user to share registries in order to ease the overhead of the host centric IDM by registering users only one time but enabling them to obtain access to various systems. The example below also shows **how** the model performs outcome by responding to client's request in Centralized IDM environment.

Source: http://www.intelligententerprise.com/showArticle.jhtml?articleID=54200324#

Figure 9 Example of responding to client to fulfil request securely in centralized IDM

The above figure 7 suggest that it is when initiating client logs on desktop that enables the client to be authenticated through the local authority LDAP as defined in figure 7. The process of logging on to the desktop enables the client to pass a request which consist of returned authentication information to the SAML service, while wrapping the information in the token generated by SAML by sending query to the LDAP. Once the query is verified, the web service permits access to the data resource. The web service then fulfils the client's request by sending the response back.

2.6.1 TRUST IN CENTRALIZED IDM

Trust management in the Centralized IDM is based on the trust method ***"Third Party authentication"*** in which trust is managed through a single host system for an entire Network. In such environment the single host system is trustworthy for keeping Identity information in its registry of all participating entities such as users, involved systems, and applications.

In this environment there is no direct relationship between any existing entities, while there is relationship between the Third Party authentication services. Trust in such condition is

established on the basis of secret sharing between each entity via the Third Party authentication service [Benantar, 2006: 74-75].

2.6.2 THIRD PARTY AUTHENTICATION TRUST METHOD IN CENTRALIZED IDM

Graph (G):

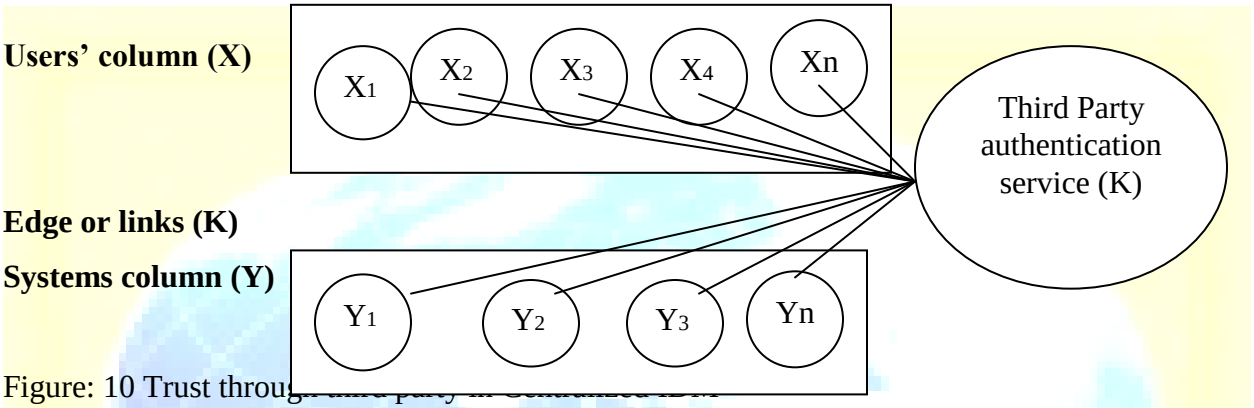

Figure: 10 Trust through third party in Centralized IDM

Source: Messaoud (2006) pg 75:

The above figure is an example that represents the Third Party authentication scheme to establish Identity Trust in Centralized IDM in which it is defined, when authentication is carried out across column [X] of users and column [Y] of involved systems; needs to manage only [X+Y] secrets, while it was [X ×Y] in Local Identity Trust Management. This means, complexity of IDM created due to [X ×Y] has been reduced to [X+Y] to establish Identity Trust relationship between Third Party and [X and Y] entities also called principals.

The above figure contains two disjoint set nodes e. g. users denoted by (X), systems denoted by (Y), graph denoted by (G) and links denoted by third party authentication (K). As the provision of establishing trust in Centralized IDM is based on sharing secret between each entity and third party authentication (K) the graph (G) forms the relationship between entities by links denoted by (K) that can be expressed as follow:

$G = \{(X + Y) \times (K)\}$

$G = \{(X \times K) + (Y \times K)\}$, where

$X = \{(x1 + x2 + x3 + \ldots\ldots\ldots xn) \times (K)\}$

$Y = \{(y1 + y2 + y3 + \ldots\ldots\ldots yn) \times (K)\}$

The equations above form the relationship based on secret sharing; e. g. password as two vertices or nodes (X and Y) in graph (G) are connected by defined path or links (K) i.e. X to K and Y to K of each other that enables it to establish trust in order to gain access for services via third party (K) and this reduces the complexity of managing trust based on ($X \times Y$) relationship to ($X + Y$). The managed trust is as follow:

$G = \{(X \times K) + (Y \times K)\}$

$G = (X + Y)$

$G = \{(x1 + x2 + x3 + \ldots\ldots\ldots xn) + (y1 + y2 + y3 + \ldots\ldots\ldots yn)\}$

2.7 EXISTING STANDARD/MECHANISM OF TRUST AND IDM

According to Shim et al (2005) trust and identity management is driven by the defined policies and agreements on how to share business organization's information securely and safely. This means that sharing and exchanging any individual's personal data should also take place according to the defined federal rules and regulations. Shim further states that IDM standards are based on the extensible mark-up Language (XML), which enables us to exchange identity information in cross-domains as well as inter-domain systems.

According to Benantar (2006: 113), XML is self-dependent data format in any environment e. g. software and hardware that governs and describes information by using its tags, while enabling authentication, data integrity, non-repudiation support for various signed data, with the help of its digital signature.

Benantar (2006: 114), maintaining confidentiality while defining the processing rules for its implementation to wide range of data is made possible with the XML encryption. However, exchanging information with important and specific goal needs an effective protocol such as SOAP. SOAP is a lightweight protocol that provides a simple messaging framework supplying extensibility, while enabling to exchange identity information in a decentralized or Network/Distributed IDM environment.

2.8 Concluding Remark

The place of Trust and Identity Management in any establishment cannot be over emphasised considering the level of knowledge from the various literature of different authorities in the area. Essentially, the literature review discusses the various concepts of IDM, the different models of IDM. Discussion of their benefits and limitations were also contained in the literature review. Most importantly is that, the opinions and works of the different scholars discussed in the literature review reflect almost similar scenario with respect to the application of Trust and IDM. By and large, the role of Identity management in an organization cannot be over emphasized as it is bedrock to dealing with Identity conflict. The literature review has provided enough lessons to the reader; as well as an ample knowledge and workability of IDM.

References

Benantar, M. (2006) *Access Control System: Security, Identity Management and Trust Models*, New York: Published by Springer.

Butler Group (2006) Identity and Access Management-Laying the Foundations for a Trusted Business Environment. Identity Management Technology; *Establishing Identity – The Dual Role of Identity Management.* Published in the UK. Published by Butler Direct Limited

Cunningham, P. & Cunningham, and M. (2006) Exploiting the Knowledge Economy: Issues, Application and Case Studies. [Online], Published in Washington, DC: IOS Press Online. http://books.google.co.uk/books?id=q3ZTVtnNb9IC&pg=PA676&dq=Network+identity+management+model&sig=UTUQunI-C8kPyO4FEDIiQet-AWQ#PPA676,M1, [Accessed 9th January 2008].

Fuchs & Pernul (2007) Supporting Complaint and Secure User Handling – A Structured Approach for In-House Identity Management. Paper presented at the IEEE International Conference on Availability, Reliability and Security, Regensburg, Germany. [Online] http://0-

ieeexplore.ieee.org.lispac.lsbu.ac.uk/iel5/4159773/4159774/04159826.pdf?tp=&arnumber=4159826&isnumber=4159774, [Accessed 22nd January 2008]

Hatala, M. and Gasevic, D. (2007) Enabling User Control with Personal Identity Management. Paper presented at the IEEE International Conference on Services Computing, Canada. [Online] http://0-ieeexplore.ieee.org.lispac.lsbu.ac.uk/iel5/4278609/4278610/04278638.pdf?tp=&arnumber=4278638&isnumber=4278610, [Accessed 22nd January 2008]

Li, H. & Singhal, M. (2007) Trust Management in Distributed Systems. [Online] Available from: http://0-ieeexplore.ieee.org.lispac.lsbu.ac.uk/iel5/2/4085604/04085622.pdf?tp=&arnumber=4085622&isnumber=4085604, [Accessed 9th February 2008]

Shim et al (2005) *Federated Identity Management* [Online] Available from: http://0-ieeexplore.ieee.org.lispac.lsbu.ac.uk/iel5/2/33102/01556498.pdf?tp=&arnumber=1556498&isnumber=33102,
[Accessed 22nd January 2008].

Thompson, R. D. & Thompson, W. C. (2007); Architectural Perspectives. Identity Management. [Online] Available from: http://0-ieeexplore.ieee.org.lispac.lsbu.ac.uk/iel5/4236/4196161/04196180.pdf?tp=&arnumber=4196180&isnumber=4196161, [Accessed 22nd January 2008]