INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211

Online Identity Management Techniques: Identification and Analysis of Flaws and Standard Methods

Aparajita Pandey
Assistant Professor, Department of EEE,
BIT (MESRA), Jaipur Campus, Jaipur, Rajasthan, India

Dr. Jatinderkumar R. Saini
2Director (I/C) & Associate Professor,
Narmada College of Computer Application, Bharuch, Gujarat, India

Abstract:

Cyberspace, and the technologies that enable it, allow people of every nationality, race and point of view to communicate, cooperate, and prosper like never before. Today as nations and people use the networks that are all around us, everyone has to work together to realize the potential for greater prosperity and security or we will succumb to narrow interests and undue fears that limit progress. Internet is one of the best examples of a self organized community as society, academia, private sector and government work together for its effective management. We have to build a cyberspace which is open, interoperable, secure and trustworthy. We have studied the related literature and in this paper, we present and discuss the flaws identified in the Identity Management processes. We also discuss the techniques which are proposed or implemented for the online Identity Management. A special attention is also given to the implementation perspective of the proposed Trust Model for India.

Keywords: Identity Management, Online Identity, Privacy

Introduction:

Never has online identity and privacy been more important than today, in the age of the Internet, the World Wide Web and smart phones. Much of the innovation is enabled by novel uses of personal information. So, we have to do what we have been doing in the past: apply our timeless privacy values to the new technologies and circumstances of our times.

Trust is essential to maintain the social and economic benefits that networked technologies bring to the world. With the confidence that companies will handle information about them fairly and responsibly, consumers have turned to the Internet to express their creativity, join political movements, form and maintain friendships, and engage in e-commerce.

Privacy protections are critical to maintaining consumer trust in networked technologies. When consumers provide information about themselves—whether it is in the context of an online social network that is open to public view or a transaction involving sensitive personal data—they reasonably expect companies to use this information in ways that are consistent with the surrounding context. Many companies live up to these expectations, but some do not. Neither consumers nor companies have a clear set of ground rules to apply in the commercial arena. As a result, it is difficult today for consumers to assess whether a company's privacy practices deserve their trust. Key challenges towards the development an Identity Management System are to tackle the conflicting requirements of privacy, identification and security.

Digital identity corresponds to the electronic information associated generally with an individual in a particular identity system. Identity systems are used by online service providers to authenticate and authorize users to services protected by access policies. Having good identity systems can enable individuals to use effectively and extensively electronic transactions in a secure yet privacy preserving manner. With the advent of distributed computing models such as web services, the current trend is to focus on inter-organization and inter-dependent management of identity information, rather than identity management solutions for internal use [1].

THE FLAWS OF IDENTITY MANAGEMENT (IDM)

To succeed in the marketplace, identity management systems must engender the trust of users and Relying parties (RP). To do so, they must improve security, control the flow of personal information, and, most important, simplify the processes of authentication, identification, and assertion of credentials. Identity management systems' scale and complexity, combined with the privacy and security requirements demanded of them, create steep challenges for usability. In this article, we posit seven flaws or design challenges that must be met for the general public to accept and use identity management systems. The challenges involve dependencies, complex trade-offs, and sometimes even contradictory design requirements, and therefore must be addressed in an integrated fashion.

Identity management –Seldom a Primary Goal

Users want many of the benefits of a well-designed identity management system, such as increased privacy or security. But, users are unwilling to invest time or money in security improvements [2].

Users follow the path of least resistance

Systems are more likely to be adopted if they're easy to download, install, and configure. This includes the authentication process and password interfaces, which must become as easy as today's standard login to successfully compete. When technology interferes with desired activities, users devise shortcuts, often undermining security in the process. For example, users might share credentials or use multiple identities when they should only use one. Ironically, attackers are experts in usability—they know how to exploit users' lack of understanding and their tendencies to use shortcuts by developing social engineering attacks to steal identity information. For identity management systems to succeed, users must find them easy to correctly and securely configure and use. It's also important to integrate identity management into the operating system or browser, so that users don't need additional software or incur additional costs.

Cognitive Scalability vs. Technical Scalability

Today, users face a burden of managing their increasing number of identifiers. This is evident by so-called "password fatigue." On average, users have approximately 25

accounts that require passwords, and they type eight passwords per day [3]. To reduce their memory burden, they choose the same or similar passwords for their various accounts and, when possible, choose the same or similar login names [3, 4].

Too many warning messages could lead to maximum information disclosure

When users encounter security warning messages, installation screens, or end-user license agreements, they tend to quickly skim the text and efficiently and they rarely understand what they have consented to [5, 6]. Furthermore, they become habituated to warnings and cease paying attention after seeing a warning multiple times. Users also ignore similar but different warnings, even when displayed in different situations. If users are asked to consent to releasing information through easily dismissed mechanisms, they might agree if it's the most convenient way to reach a goal, regardless of whether that action is in line with their privacy and security concerns.

Asking users to consent to more transactions won't result in greater control of information disclosures in identity management systems. By asking them to manage more identity information and presenting them with more choices, they are only overwhelmed. The end result could be a system that increases, rather than minimizes, the identity data that users are willing to reveal to third parties [7].

Mutual Authentication

Many identity management systems focus primarily on user authentication. Phishing attacks have illustrated that it's equally important for the user to be able to authenticate the Identity Provider (IdP) and Relying Party (RP). This requirement applies to any system in which a credential can be discovered and reused, particularly when attackers can spoof an IdP. With today's software and authentication systems, identity attacks are trivial to launch. Attackers can easily simulate Web site user interface elements, including content and security indicators that site or software applications might present. Most users can't distinguish a legitimate Web site from an illegitimate phishing or pharming one that's designed to capture identity data and credentials [8, 9]. One empirical study of password use observed that 1.5 percent of users submit passwords to phishing Web sites annually [10].

Federated identity systems that let users leverage one credential across many sites will only increase the value of the credential as a phishing target. To ensure that users aren't providing their passwords to a phishing site, they must be able to authenticate the RP Web site to ensure that it can be trusted to redirect to the correct IdP, and they should also authenticate the IdP's Web site. Unfortunately, there's no guarantee that a RP that behaves well today will continue to do so tomorrow; a site could build up trust and then abuse it.

From an attacker's perspective, redirect-based identity management creates the ideal infrastructure for phishing. These systems not only increase the credential's value, they also introduce a complicated new authentication procedure, train users to give their credentials to third parties, and double the number of Web sites that users must trust. Protocols must support mutual authentication (the IETF's current authentication standards for HTTP don't currently support mutual authentication. User interfaces must be difficult to spoof and should help the users to know that they are communicating with the intended party, both when authenticating directly and when using a leveraged identity. Today's interfaces and security indicators are inconsistent across browsers and operating systems, increasing the risk of user error due to unfamiliarity;4 industry cooperation and standards efforts, such as those coming from the W3C Web Security Context Working Group, could help remedy this problem.

Trustworthiness of a Web Site

Who should users trust with their identity information? Deciding who to trust is a difficult decision involving risk assessment. Unfortunately, people aren't good at risk assessment, particularly where privacy and security decisions are concerned.6

Authentication schemes, even those that security experts currently recommend and responsible organizations use, can be flawed, attacked, or poorly implemented. Even legitimate and established organizations make mistakes and lose control of databases with sensitive data such as credit-card and social security numbers [11]. In fact, managers of an identity fraud protection company have occasionally been convicted of fraud and identity theft.

IdPs have differing privacy policies and business models. Although some are focused on preserving the privacy and unlink-ability of transactions, others don't guarantee that a user's transactions will remain private. Differing policies add to the challenges users face

when verifying an IdP's trustworthiness. No one organization can ensure a completely trusted system, and any bad or careless actor can tarnish the reputation of many. Thus, the identity community as a whole has a responsibility to behave securely and call attention to practices that threaten privacy or are unsafe. Because of the central position they hope to hold in the online environment, designers and implementers of identity management systems must be extra vigilant about security risks. Before deploying systems common trust models should be developed with policies that benefit users and RPs.

RELATED STANDARD WORKS IN IDM

ITU NGN

Identity management is under development by a Focus Group on Identity Management (FG IdM) of ITU-T NGN GSI (SG13). NGN User Identity (NUI) shall provide the following functionalities [12].

• A way for a NGN user to access telecommunication services anywhere, anytime and at any terminal on the basis of a personal identifier for a network/service;

• A way for others to refer to a user as a target for terminating services (e.g., voice calls), information queries, and other NGN services, e.g., context-awareness information;

• Ability to identify, authenticate and possibly authorize the NGN user in order to protect the user's privacy and to secure the user's personal information; Enabling a network/service provider to provide those services delineated in a user's profile, e.g., addressing, routing and charging of user's calls;

• The use and type of NUI may be tied to a specific set of NGN services. An identifiable NUI includes one or two of the following NUI types: a public user identity, which shall be visible to other users and enables the information used by a NGN user to contact or communicate with another NGN user, and a private user identity in which the information used shall not be visible to other users and can identify a NGN user to a user's network/service provider.

NGN shall support selective authorization of attribute information (e.g., identity lifetime) by an attribute provider and allow separate identification, authentication and authorization of users and terminal equipment. NGN shall also support a dynamic binding of user identity and terminal equipment (identity) and allow the association of a user identity to support multiple terminal equipment (identities) for certain services. A

service provider may allow a user to access a service from multiple terminals in parallel using the same public and private user identities.

EIS and ETSI

The European Information Society (EIS) requires technologies which address trust and security yet also preserve the privacy of individuals. As the EIS develops, the increasingly digital representation of personal characteristics changes our way of identifying individuals. Supplementary digital identities, so-called virtual identities, embodying concepts such as pseudonymity and anonymity, are being created for security, profit, convenience or even for fun. These new identities are feeding back into the world of social and business affairs, offering a mix of plural identities and challenging traditional notions of identity. At the same time, European states manage identities in very different ways. ETSI, European Telecommunications Standards Institute, is developing a Universal Communication Identifier (UCI). This concept, as originated in 2000, is being considered for use in NGN [13]. Traditional identifiers are bound to communication services (e.g. E.164 numbers to telephony services and e-mail addresses to e-mail service providers). UCIs are bound to Personal User Agents (PUAs) that negotiate with other PUAs to deliver communication services configured to the needs of both parties. Each UCI user has a PUA, which is permanently available, and acts as a proxy for the user within the ICT environment. PUAs have the following functionalities [14].

- Access to a list of the user's contacts;
- Access to all of the user's information and communication preferences;
- Contains rules that control how users wish their communications to be managed;
- Negotiating with other PUAs to try to achieve a mutually acceptable outcome.

With UCI, people can exert fine control over how they handle unsolicited communications. UCI needs Service Agent (SA) functionality to ensure that PUAs have a standardized interface to all applications, services and networks. This SA functionality could require little or no changes to some existing APIs and gateways. In other cases, SA functionality could require some form of specialized middleware.

If UCI and the supporting PUAs and SAs are deployed, they provide a platform from which a number of new value-added capabilities can easily be built. Such capabilities

include protection from spam and phishing attacks by trusting only 'authentic' identities and a potential to meet a wide range of user preferences e.g., type of communication, language, high availability and do-not-disturb periods. The UCI has at least the following 6 properties:

a) an identifier must be resolvable to identify a unique resource,

b) if it is to be used universally, all systems must be able to transport and decode it,

c) it must be structured,

d) it would be beneficial if existing systems can process it without significant update,

e) a numeric element conforming to the E.164 scheme easily meets all of the above criteria,

f) additional data elements can be used to convey information such as whether the UCI label is 'authentic' or not, the preferred language for the information or communication session and special user requirements e.g. textual information presentation for a deaf user.

UCI maps to NGN via the following ways:

a) early UCI work described requirements and defined a conceptual architecture,

b) mapping to concrete environments with easy no pre-defined technology choices and examining if available services deliver required functionality and

c) examining how NGN system entities, protocols and services (e.g. SIP, Presence and ENUM) can deliver the capabilities required by UCI.

GPP

TS23.003 [15] of 3GPP defines the principal purpose and use of International Mobile station Equipment Identities (IMEI) within the digital cellular telecommunications system, which includes an identification plan for [15] 3GPP TS 23003, Numbering, addressing and identification, version, 7.1.0, 2006-09

• mobile subscribers in the GSM system,

location areas, routing areas, and base stations in the GSM system, MSCs, SGSNs, GGSNs, and location registers in the GSM system,

• point-to-multipoint data transmission groups,

• CN domain, RNC and service area in the UTRAN system,

• groups of subscribers to the Voice Group Call Service (VGCS) and to the Voice Broadcast Service (VBS),
• voice group calls and voice broadcast calls,
• group call areas for mobile subscribers in the WLAN system,
• assigning Packet Data Protocol (PDP) addresses to mobile stations, and a group of principles of
• assigning IMEIs,
• assigning telephone and ISDN numbers to MSs (Mobile Stations) in the country of registration of the MS,
• assigning MS roaming numbers to visiting MSs,
• assigning zones for regional subscriptions.

Liberty Alliance

Liberty Alliance proposes a Liberty Identity federation framework, which consists of a service provider and an identity provider to offer a viable approach for implementing SSO with federated identities, which identity provider would be required to support the SSO protocol, and one or more profiles that use that protocol. The aim of the federated network identity is to reduce the identity fragmentation across various identity providers and realize new business taxonomies and opportunities, coupled with new economies of scale.

The first time that users use an identity to log in to a service provider they must be given the option of federating an existing local identity on the service provider with the identity provider login to preserve existing information under the SSO. The single logout protocol provides a message exchange protocol by which all sessions provided by a particular session authority are near-simultaneously terminated. The single logout is used either when a principal logs out at a session participant or when the principal logs out directly at the session authority. This protocol may also be used to log out a principal due to a timeout. The reason for the logout event can be indicated through the reason attribute [16].

LID and OpenID.

LID (Light-Weight Identity) [17] and OpenID [18] originated from different places but today interact using the Yadis platform [19]. There is no a priori trust associated with

the underlying protocols. The home site (identity provider) can be owned/administered by the user itself. They work as a sort of reputation mechanism.

Yadis is the underlying service discovery infrastructure for users, it "allows software to declare, and determine supported by any given identity or Relying Party URL".

These URLs are the identifiers for the personas (or identities) used both in OpenID and LID. They enable a user to authenticate at a HomeSite that the service being accessed does not need to trust (in a cryptographic sense) and that the user is allowed to own/administer. The use of URLs as identifiers allows them to be easily searched using current web search engines. The URLs point to the server that can verify the user's credentials.

In LID the URL can have commands to retrieve/query specific persona attributes, edit these attributes, etc. There is also the provision to use signatures in these commands, thus providing some form of crypto trust. These signatures are based on web-of-trust models, as for example PGP (Pretty Good Privacy).

SXIP.

SXIP (Simple eXtensible Identity Protocol) [20] is based on DIX (Digital Identity Exchange Protocol). DIX is an effort to standardize the protocol at the IETF. Sxip adds the possibility for some of the persona attributes being validated by a trusted 3rd party. For example one could have an email certified by VeriSign. The services can define attributes that are optional on an if-available basis. This means that if the HomeSite can provide the attributes (they are already stored) it will, but if it does not have them it will not ask the user for them. As before, the user controls what attributes are released to the Relying Parties [20].

LDAP

LDAP (Lightweight Directory Access Protocol) [21] is a promising technology that provides access to directory information using a data structure similar to that of the X.500 protocol. IBM Tivoli, Novell, Sun, Oracle, Microsoft, and many other vendors feature LDAP-based implementations. The identities managed through this framework can have digital signatures either by the underlying context or provided by components of the framework. These components resort to I-Card providers that have trust relationships with Service Providers. Microsoft tries to lay some basis for their Infocard

system [22]. It relates to the user-centric federation toolkits due to its aim for interoperability with other systems and the premise of giving the user control of her identities, as mentioned in [22]: "credit card providers might issue identities enabling payment, businesses might issue identities to their customers, governments might issue identities to citizens, and individuals might use self-issued identities in contexts like signing on to Web sites."

VID

To match this purpose, European IST (Information Society Technology) integration project Daidalos [23] is developing a new global identity, in terms of a Virtual Identity (VID), which operates across all network cross layers and intra and/or federated inter domains. [23] Daidalos IST Project: Daidalos: "Designing Advanced Interfaces for the Delivery and Administration of Location independent Optimised personal Services". (IST-2004-026943). The VID framework presents a new paradigm in computer communication systems. In order to keep up with present times, when access to the Internet and other communication infrastructures and services are no longer a privilege of the few, a VID opens the door to online identity VID contemplates a multitude of identities and roles that we take on each time we turn on our computer, mobile phone or PDA. Since all the attributes are part of a user, the attributes should be under the user's control and not under the control of the network. As a user, a person has a right to control how much of his personal data is given to the services he accesses, especially if that data is not absolutely necessary.

Under all these assumptions on rights and duties of the users, their services and the networks, the VID framework is bound to law, presents its users with a range of new and interesting possibilities in the fields of privacy, identity and federation.

Users are not the only ones who can have several identities. In fact, any entity capable of establishing legal relationships with other entities can benefit from this framework. We propose that users, groups, service providers, network operators and even banks all share this identity framework and use it to communicate with each other and establish their relationships, not based solely on their 'real' but also on their 'virtual' identity.

AADHAAR

Aadhaar [24] is a 12 digit individual identification number issued by the Unique Identification Authority of India on behalf of the Government of India. This number will serve as a proof of identity and address, anywhere in India. Any individual, irrespective of age and gender, who is a resident in India and satisfies the verification process laid down by the UIDAI, can enroll for Aadhaar. Each individual needs to enroll only once which is free of cost. Each Aadhaar number will be unique to an individual and will remain valid for life. Aadhaar number will help you provide access to services like banking, mobile phone connections and other Government and Non-Government services in due course. Aadhaar will be:

- Easily verifiable in an online, cost-effective way
- Unique and robust enough to eliminate the large number of duplicate and fake identities in government and private databases
- A random number generated, devoid of any classification based on caste, creed, religion and geography

Privacy Laws In India

India is not a particularly private nation. Personal information is often shared freely and without thinking twice. Public life is organized without much thought to safeguarding personal data. In fact, the public dissemination of personal information India does not currently have a general data protection statute. Nevertheless, the judiciary has derived a "right of privacy" from the rights available under Articles 19 (1) (a) (the fundamental right to freedom of speech and expression) and 21 (the right to life and personal liberty) of the Constitution of India. However, all cases that deal with the right to privacy have been decided in the context of Government actions that resulted in private citizens being denied their right to personal privacy. No privacy judgment has granted private citizens a right of action against the breach of privacy by another private citizen. To that extent, the data protection and personal privacy jurisprudence in the country is not yet fully developed.

Personal information is often shared freely and without thinking has over time, become a way of demonstrating the transparent functioning of the government. While many agencies of the government collect personal data, this information is stored in silos with

each agency of the government maintaining information using different fields and formats. Government databases do not talk to each other and given how differently they are organized, the information collected by different departments cannot be aggregated or unified Data privacy and the need to protect personal information is almost never a concern when data is stored in a decentralized manner. Data that is maintained in silos is largely useless outside that silo and consequently has a low likelihood of causing any damage. However, all this is likely to change with the implementation of the UID Project. One of the inevitable consequences of the UID Project will be that the UID Number will unify multiple databases. As more and more agencies of the government sign on to the UID Project, the UID Number will become the common thread that links all those databases together. Over time, private enterprise could also adopt the UID Number as an identifier for the purposes of the delivery of their services or even for enrollment as a customer. Once this happens, the separation of data that currently exists between multiple databases will vanish. Such a vast interlinked public information database is unprecedented in India. It is imperative that appropriate steps be taken to protect personal data before the vast government storehouses of private data are linked up and the threat of data security breach becomes real. Similarly, the private sector entities such as banks, telecom companies, hospitals etc are collecting vast amount of private or personal information about individuals. There is tremendous scope for both commercial exploitation of this information without the consent/ knowledge of the individual consent and also for embarrassing an individual whose personal particulars can be made public by any of these private entities. The IT Act does provide some safeguards against disclosure of data / information stored electronically, but there is no legislation for protecting the privacy of individuals for all information that may be available with private entities.

In view of the above, privacy of individual is to be protected both with reference to the actions of Government as well as private sector entities [25].

Conclusion

Today, on the Internet, users' digital identities are independently managed by different platforms in different security domains. This causes 'identity fragmentation'. This problem leads users to have an inconvenient and inconsistent experience when they use IT or network services. However, user information privacy and security are becoming more and more important.

To meet the goals of building trust, improving security, reducing fraud, and simplifying users' lives, identity management systems must be designed in a truly user-centric method. This requires that they learn from existing literature about usable security and privacy and take cognitive and technical limitations equally into account when placing demands on users. Poorly designed identity management systems can aggravate existing security problems and create greater opportunities to extract personal information from users.

A good Identity Management System should have the following properties:

1. Security and identity management are secondary goals. Identity management should be integrated into the browsers, operating systems, and applications people already use, and make it easy for them to configure and operate systems correctly.
2. The number of trust decisions users has to make should be decreased. The users should not be overwhelmed with more warnings, dialogs, and indicators.
3. Mutual authentication should be there between the users and the web sites they visit to help users detect spoofing attacks.
4. To increase the awareness about the privacy issues to the users, workshops and training should be organized.
5. Common Trust Models should be developed on which users and relying parties will agree to participate.

By replacing single-site identity silos, Web scale identity management systems have a great potential to improve security and simplify users' online interactions. There are many stake-holders as well as conflicting requirements, so designers must always look at the big picture. Systems providers are already experimenting with different technical approaches and making different choices about trade-offs. To become a ubiquitous and well-understood technology, identity systems must integrate seamlessly into Web sites, be natively supported by Web tools, and strike the right balance between usability, privacy, and security.

REFERENCES

[1] Andre Durand, "How the Nature of Identity Will Shape Its Deployment" Nov/Dec 2003, DigitalWorld. http://www.digitalidworld.com/misc/LayersofIdentityArticle.pdf

[2] .A. Acquisti and J. Grossklags, "Privacy and Rationality in Decision Making," IEEE Security & Privacy, vol. 3, no. 1, 2005, pp. 26–33.

[3] D. Florencio and C. Herley, "A Large Scale Study of Web Password Habits," Proc. Int'l Word Wide Web Conf. (WWW 07), ACM Press, 2007, pp. 657–665.

[4] R. Dhamija and A. Perrig, "Déjà Vu: A User Study—Using Images for Authentication," Proc. 9th Usenix Security Symp., Usenix Assoc., 2000, pp. 45–58.

[5] N. Good et al., "Stopping Spyware at the Gate: A User Study of Privacy, Notice, and Spyware," Proc. Symp. Usable Privacy and Security (SOUPS 05), ACM Press, 2005, pp. 43–52.

[6] J. Grossklags and N. Good, "Empirical Studies on Soft--ware Notices to Inform Policy Makers and Usability Designers," Proc. Usable Security (USEC 07), Lecture Notes in Computer Science, Springer, 2007.

[7] B. Schwartz, "The Tyranny of Choice," Scientific Am., Apr. 2004, pp. 71–75.

[8] R. Dhamija, J.D. Tygar, and M. Hearst, "Why Phishing Works," Proc. Conf. Human Factors in Computing Systems (CHI 06), ACM Press, 2006, pp. 581–590.

[9] S. Schechter et al., "The Emperor's New Security Indicators," Proc. IEEE Symp. Security and Privacy, IEEE CS Press, 2007, pp. 51–65.

[10] D. Florencio and C. Herley, "A Large Scale Study of Web Password Habits," Proc. Int'l Word Wide Web Conf. (WWW 07), ACM Press, 2007, pp. 657–665.

[11] Privacy Rights Clearinghouse, Chronology of Data Breaches, www.privacyrights.org/ar/ChronDataBreaches.htm.

[12] Pierre André Probst, an ITU-T initiative towards global standards on Network Aspects of Identification Systems, Identity workshop of ITU, 2006-12.

[13] ETSI TS 184002: TISPAN, Identifiers for NGN, Version: 1.1.1, 2006-06.

[14] Mike Pluke, Universal Communications Identifier (UCI) – Trusted, Meaningful Identification, Identity workshop of ITU, 2006-12.

[15] 3GPP TS 23003, Numbering, addressing and identification, version, 7.1.0, 2006-09

[16] Liberty Alliance, Liberty ID-FF architecture overview, version 1.2, 2004-09.

[17] Light-WeightIdentity™LID, http://lid.netmesh.org/wiki/Main_Page

[18] David Recordon, Brad Fitzpatrick, "OpenID Authentication 1.1", (http://www.openid.net).

[19] Joaquin Miller (ed), Yadis Specification, Version 1.0, 18 March 2006 (http//www.yadis.org).

[20] Sxip Specifications and Documents, http://www.sxip .net/Specs.

[21] M. Wahl, T. Howes, and S. Kille, "Lightweight Directory Access Protocol (v3)," IETF RFC 2251, Dec. 1997; www.ietf.org/rfcrfc2251.

[22] Microsoft Whitepaper, "Microsoft's Vision for an Identity Metasystem", http://www.identityblog.com/ stories /2005/07/05/IdentityMetasystem.htm.

[23] Daidalos IST Project: Daidalos: "Designing Advanced Interfaces for the Delivery and Administration of Location independent Optimised personal Services". (IST-2004-026943). Available http://www.ist-daidalos.org.

[24] http://uidai.gov.in/aadhaar-usage.html

[25] http://www.prsindia.org/uploads/media/UID/aproach_paper.pdf