International Journal of Engineering Innovation & Research
Volume 1, Issue 2, ISSN : 2277 – 5668

An Investigation of Challenges to Online Federated Identity Management Systems

Aparajita Pandey
Assistant Professor, Department of EEE,
BIT (MESRA), Jaipur Campus, Jaipur, Rajasthan, India
aparajitasp@rediffmail.com

Dr. Jatinderkumar R. Saini
Associate Professor & I/C Director,
Narmada College of Computer Application, Bharuch, Gujarat, India
saini_expert@yahoo.com

***Abstract* — National and global economic, governmental and social activities now rely more and more on the Internet. Online Identity Management (IdM) is a crucial component of those activities. Today, organisations in both the public and private sectors vary significantly in their approaches to IdM, devising their own means for establishing, verifying, storing and using digital identities over their networks and the Internet. Thus, the lack of common policies and approaches to such Federated IdM systems creates privacy, security and productivity issues in the increasingly interconnected economies, and hampers the ability of organisations to provide users with convenient services. This paper presents the investigation and discussion of challenges faced in implementing the Federated IdM in the online system. Also, a trust-based framework is discussed in order to combat these challenges**.

***Key Words* — Authentication, Authorization, Federated Identity Management, Identity Theft, Single Sign-on (SSO), Trust Framework**

I. INTRODUCTION

Verifying the identity of a person or entity who seeks remote access to a corporate system, who communicates through an e-mail, or who signs an electronic document, is the domain of what has also come to be called Identity Management (IdM). It is increasingly playing a critical role in online commerce. The European Commission [1] has defined it as, 'Electronic Identity Management is a key element for the delivery of any e services. On the one hand, e-identification gives individuals using electronic procedures the assurance that no unauthorized use is made of their identity and personal data. On the other hand, administrations are able to make sure that the individuals are the persons they claim to be and have the rights that they claim to have (e.g. to receive the requested service)'. The OECD [2], in its Recommendation on Electronic Authentication, has expressed a similar view. It says that electronic authentication provides a level of assurance as to whether someone or something is who or what it claims to be in a digital environment. Thus, electronic authentication plays a key role in the establishment of trust relationships for electronic commerce, electronic government and many other social interactions. It is also an essential component of any strategy to protect information systems and networks, financial data, personal information and other assets from unauthorized access or identity theft. Electronic authentication is therefore essential for establishing accountability online.

Identity Management is also critical in information security. It is the basis for most types of access control and for establishing accountability online. Thus, it contributes to the protection of privacy by reducing the risks of unauthorized access to personal information, data breaches, and identity theft. The critical importance of online Identity Management in facilitating trustworthy ecommerce and ensuring national security is now well recognized. Several other governments and inter-governmental forums are already actively working to address the applicable technical and legal issues. These include Australia, Canada, the EU, India, the OECD, Scotland and the United States [3, 4, 5, 6, 7, 8].

The OECD [2] defines Identity Management (IdM) as: "The set of rules, procedures and technical components that implement an organization's policy related to the establishment, use and exchange of digital identity information for the purpose of accessing services or resources. Effective IdM policies safeguard digital identity information throughout its life cycle – from enrolment to revocation – while maximizing the potential benefits of its use, including across domains to deliver joined-up services over the Internet."

Without adequate Identity Management, the need to identify persons seeking online access is complicating life for individual users (who must remember many User IDs and passwords), and is becoming increasingly costly for businesses who must identify and authenticate the ever-growing number of persons and entities with whom they deal electronically. In addition, it increases privacy risks to the individuals being identified, especially as more and more entities collect and exchange an ever-increasing amount of personal data from and about such individuals, all in the name of Identity Management.

A typical IdM proposes to provide authorization based on the authentication of the entity. This concept is extended to provide similar kind of authentication-based authorization to multiple resources at the level of a single organization. This concept is further extended to multiple organizations through Federated Identity Management (Federated IdM) Systems. Federated IdM [9], in general, is one of the ways to authenticate the Identity in online world. It allows people to outsource the identification and authentication process to a third party and simplifies the process for users by allowing them to use a Single Sign-on (SSO).

In this paper the challenges faced in implementing the Federated IdM in the online system are discussed. This is followed by the discussion of how these challenges can be

overcome. To understand Federated Identity Management and the challenges, first, we review the basic processes involved in Identity Management.

II. BASICS OF IDENTITY MANAGEMENT

The underlying processes of Identity Management have been in use in an offline environment. Passports, driver's licenses, and employee ID cards, voter ID cards, are all components of what might be referred to as Identity Management systems – i.e., they are credentials issued by an entity for the purpose of identifying individuals, and they are used by such individuals to validate their identity in order to enter into a transaction with a third party. While there are many different approaches to Identity Management, it essentially involves three fundamental processes [8]:

(1) The process of identifying a person and issuing an identity credential to reflect that identity ("identification")
(2) The process of later verifying that a particular person presenting that credential and claiming to be that previously identified person is, in fact, such person ("authentication")
(3) Once an individual's identity is successfully authenticated, a third process, referred to as "authorization," is used by the business relying on the authenticated identity to determine what rights and privileges are accorded to such person ("authorization")

The challenge is to import a similar approach to the digital online environment. That is, to create secure, reliable and trustworthy digital identity credentials that can be used across different systems and environments. This allows individuals to use the same identity credential to sign on to the networks of more than one business in order to conduct transactions.

III. THE CHALLENGES FOR FEDERATED IDM

The challenges of any Identity Management system fall into three general categories [9]. First are the technological, process, and procedural challenges, such as implementing the required technology and establishing appropriate processes and procedures so that everything works properly, ensuring the inter-operability [10] of identity information communications between Identity Providers and Relying Parties, and ensuring the security of Subject identity information. The second challenge is economic, and involves primarily dealing with the cost of deploying, coordinating, and using Identity Management systems. The third challenge is legal. It focuses on issues relating to the potential liability risk of the participants, the privacy and security of the Subject's identity information, and the mutual concerns of all participants (Subject, Identity Provider, and Relying Party) that everyone performs their obligations properly. The legal risks to each participant in an identity system, and the significance of those risk will, of course, vary by the role such participant is fulfilling at any particular point in time. In addition to above classification, we have found that they fall into the following general categories:

A. Technology Related Challenges

Identity Management relies on a variety of different technologies. These might include, technologies used to create and secure data on various credentials and tokens, encryption technologies, data security technologies, etc. While the technologies used in any given identity system will vary, it is critical to the operation of the system that the technologies utilized are appropriately designed to achieve the intended result, that they function properly and securely, and that they provide reliable and secure results. Thus, one key challenge to the participants in an identity system is the risk that one or more of the technologies employed for a particular IdM system do not function properly and/or do not achieve the intended result.

B. Process Related Challenges

In addition to technology, Identity Management relies on a variety of different processes and procedures, some of which are not technology-based, but rather consist merely of a series of steps performed by a person. Such processes and procedures might include, for example, the process for identity proofing an individual Subject, which might specify which identity documents must be reviewed in person, or how identity might be verified online. Other processes relate to authentication, verification of credentials, revocation of credentials, etc. Like the technology, it is critical that the processes and procedures work properly. For example, is the identity proofing process adequate to yield a trustworthy identification result? Thus, another key risk to the participants in an identity ecosystem is the risk that one or more of the processes implemented for that particular identity ecosystem are not properly designed to yield a secure and trustworthy result.

C. Performance related challenges

Even if the technologies and processes used for an identity ecosystem are properly designed to yield a secure and trustworthy result, they will be of little value if they are not correctly implemented or properly followed by the persons responsible for using them. Thus, a key challenge for all participants in an identity system is the risk that one of the other participants, on whose performance they rely, will not perform their obligations as required for the role in which they are acting [9]. Only when this risk is reduced to an acceptable level will parties participate in an Identity Management system. Thus, for example, the security agent at an airport generally feels comfortable accepting the risk that a state has properly identified each person to whom it has issued a passport. If it did not, such identity credentials would not be accepted. To alleviate this risk requires clearly defining the performance obligations of each role, utilizing a mechanism (e.g., statutory, contractual, and/or technological) to provide some assurance that the participants in each role will perform their obligations conducting performance audits where appropriate, and providing a remedy if someone does not.

D. Challenges Related to Privacy

By its nature, any form of federated Identity Management involves the collection (by an Identity Provider) and disclosure (to a Relying Party) of personal information about a Subject. Thus, the foundational issue in approaching any Identity Management system is personal information – how it is collected, stored, shared, and used [11]. Moreover, by its nature, federated Identity Management presents a new challenge to privacy, in that transfers of personal information routinely occur between organizations as well as between the individual and an organization, and might frequently cross industry sectors and jurisdictional boundaries in the process. Privacy risk focuses on the possibility that personal data collected as part of the identity proofing process will be misused by one of the parties who has access to it (typically the identity provider and subsequent Relying Parties), or that the personal information will be compromised or otherwise improperly disclosed. Privacy risk in many respects is a function of technology risk and performance risk. However, it may go beyond those two risks in that the use or protection of the personal information in certain ways may not be required by the applicable system rules, or, in addition to the rules, may be regulated by existing law. The privacy risk for Subjects focuses on the protection and use of their personal information by Identity Providers, Relying Parties, and other third parties, the resulting possibility of inappropriate use, disclosure, and compromise, and the harms that may result, such as identity theft, unauthorized account access, embarrassment, etc. And this risk relates not only to the information provided by the Subjects, but also information about the Subjects collected from third parties, as well as metadata and transaction data about Subjects generated as a result of their online activities. For Identity Providers and Trusting Parties, the privacy risk involves navigating the challenges of compliance obligations and restrictions that might inhibit their ability to achieve their goals. Laws and regulations may regulate or restrict their collection and use of personal information, as well as impose a variety of obligations to protect the information. In addition, restrictions on cross-border transfers and other forms of use or sharing of such information may have an impact. Failure to address these obligations may result in penalties and fines, as well as potential liability for any harm suffered by the Subjects themselves.

E. Challenges related to Data Security

Data security is critical to any Identity Management system. This includes not only the security necessary to protect the personal information collected and communicated to relying parties, but also the security of the other data and corresponding processes necessary to create secure identity credentials, communicate accurate identity assertions, and verify the status of identity credentials. Thus, security risk refers to the risk that an unauthorized party obtains access to personal data or is able to otherwise compromise the overall functioning of the system. For some participants, such as identity providers and relying parties, data security risk may also relate to the possibility of a failure to comply with existing applicable law.

F. Challenges related to Liability

Things that can go wrong in an Identity Management system typically result from faulty Identification, faulty authentication, inadequate security for or misuse of personal data, or failure to follow appropriate procedures. They can lead to two primary harms. First, a Relying Party and/or a Subject may suffer damages when the Relying Party acts (a) in reliance on a false identity credential or identity assertion that it thought was valid (e.g., by granting access to, or entering into an unauthorized transaction with, an imposter), or (b) fails to act in reliance on a valid identity credential that it mistakenly believes to be false. Second, a Subject may suffer damages when (a) his or her personal information is misused or compromised by the Identity Provider or a Relying Party or other third party to whom it has been disclosed, or (b) when the Subject is improperly denied access or the ability to conduct a transaction he is otherwise entitled to do. Thus, a primary concern of all participants in any identity federation is determining who will bear the risks associated with these problems and their consequences [12]. All participants in an identity system must address the risk that they will be held liable for damages resulting from a problem from which they are deemed legally responsible. Thus, a key aspect of the liability risk is the legal uncertainty regarding the responsibility that attaches to any given action or failure to act by a participant in an identity system. This uncertainty only enhances the nature of the liability risk and in many cases has dissuaded companies from participating in an identity system.

G. Challenges Related To Enforceability

If one participant in an IdM system fails to perform as required, the other participants must consider their ability to (i) identity the fact of such failure of performance, (ii) stop and/or remedy such failure, and (iii) obtain redress and/or compensation for any losses suffered as a result. Concerns regarding each of these three elements are the focus of enforceability risk. It should be noted that this risk applies not only when something goes wrong and someone seeks to recover damages, but also in situations where a problem has not yet surfaced, but a failure of performance on the part of one or more participants puts the system at risk. For example, the failure by an identity provider to properly perform the identity proving process, even though it has not yet resulted in any inaccurate credentials, is a concern for other participants in the identity system. In such case, enforceability risk refers both to the ability to detect that problem, as well as the ability to require the participant to remedy its performance or withdraw from the system.

H. Challenges related to Regulatory Compliance

In many cases, participation in an identity system raises legal compliance issues. In some cases, those issues relate to whether the conduct of the participant complies with applicable law. For example, the manner of collection, use, and storage of personal data by the identity provider, and the subsequent receipt and use of that information by a relying party, must comply with applicable privacy laws. Acting contrary to the requirements of those laws poses a compliance risk to the participant. In other cases, participation in the identity system is, itself, done in an effort to comply with legal requirements imposed on a participant. For example, a financial institution may participate, and rely on identity credentials, in order to satisfy its legal obligations to properly authenticate persons granted online access to bank accounts and payment facilities. In such cases, whether the participant adequately satisfies its compliance obligations will depend, at least in part, on the trustworthiness of the identity systems.

IV. OVERCOMING THE CHALLENGES – THE NEED FOR A TRUST FRAMEWORK

There are many technologies and Identity Management standards to ensure that personal information moving between organizations is securely transferred and can be read and understood by the systems of all parties [13]. Encryption and digital signature technology, for example, is used to protect the security of the information flows, ensure the integrity of the identity credentials and to authenticate the Identity Provider to the Relying Party. Technical standards are critical to ensuring the inter-operability of communications across various systems and networks. Without agreement on standards, different networks and systems would be unable to talk to each other and exchange information in a manner that can be understood by either system. But as Susan Landau [14] has noted regarding the technology, "Ultimately, though, the protection here is legal, a Relying Party or Identity Provider is in a position to violate a person's privacy and technical protections can only reduce, not eliminate this risk." The ultimate goal of any identity system is to provide identity assertions that are sufficiently reliable for the intended purpose, and to do so in a manner such that all of the relevant parties are willing to participate and to rely on the results. Achieving that goal requires building a "Trust Framework" for each identity system that addresses both the operational requirements and the legal rules necessary to define a trustworthy identity system. This is sometimes referred to as the "tool and rules" of an identity system. The concept of a Trust Framework is often referred to in discussions of Identity Management systems, but usually without a detailed analysis and often in an inconsistent manner. Generally, however, a Trust Framework may be defined as follows: A Trust Framework is a set of documents developed or tailored for a specific identity system, which sets forth [15]:

(1) Operational Requirements for the identity system (such as technical and functional specifications, processes, standards, policies and rules) that have been developed to ensure the proper operation of the system and to provide adequate assurance regarding the accuracy, integrity, privacy and security of its processes.

(2) Legal Rules that govern the identity system and that make the Operational Requirements legally binding on and enforceable against the participants, regulate the content of the Operational Requirements, and define and govern the legal rights, responsibilities, and liabilities of the participants of the identity system.

The Operational Requirements of a Trust Framework will likely consist of several different components addressing a variety of key operational and policy issues. While the content and structure of these components will vary from one identity system to another, the Operational Requirements of each Trust Framework will likely include common core components, such as an identity proofing component, an authentication component, a credential management component, a privacy component, a security component, an assessment/audit component. Each component of the Operational Requirements establishes the technical specifications, processes, standards, policies, rules and performance requirements necessary to address one or more issues of importance to the operation of the identity system. Taken together they form the Operational Requirements necessary to ensure that the identity system operates properly and in a manner that all parties trust will be appropriate for the task.

The Legal Rules complete the Trust Framework by rendering the various components of the Operational Requirements binding and enforceable. The Legal Rules consist of both existing statutes and regulations (i.e., publicly-created law), and agreements between or among the participants (i.e., privately-created law). They affect the Trust Framework in three ways [15, 16]:

(1) They make the specifications, standards, and rules comprising the various components of Operational Requirements legally binding on and enforceable against each of the participants.

(2) They define the legal rights and responsibilities of the parties, clarify the legal risks parties assume by participating in the Trust Framework (e.g., warranties, liability for losses, risks to their personal data); and provide remedies in the event of disputes among the parties, including methods of dispute resolution, enforcement mechanisms, termination rights, and measures of damages, penalties and other forms of liability.

(3) In some cases, they also regulate the content of the Operational Requirements.

The Legal Rules may be set out in numerous contracts at varying management and execution layers, depending on the governance structure used. In many cases they operate with respect to issues not addressed by the existing law. Where existing laws address issues in a permissive rather

than mandatory manner, the Legal Rules may also express the choices of the parties among legally permissible alternatives. And in both cases they can have the effect of providing the legal certainty and predictability necessary to encourage participation. The relationship between the Operational Requirements and Legal Rules of a Trust Framework is similar to the relationship between a contract and several sets of technical specifications attached to the contract as exhibits. Execution of the contract is what creates a legally binding relationship between the parties; the specifications in the exhibits detail the parties' expectations of how the contract will be performed. While it might be possible for the parties to work together with reference only to the specifications, by incorporating them into a contract, the technical specifications give rise to legally enforceable rights and responsibilities. In some cases, Trust Frameworks may be developed by a single entity, often referred to as a Trust Framework Provider, which is established to provide both the Trust Framework and the governance infrastructure needed to support it. A group may establish such an entity of companies or an industry sector that require a legally binding Trust Framework in order to work together efficiently.

V CONCLUSION

The protection of the identities of individuals and organizations while conducting online transactions is crucial to protect e-commerce, promote innovation, and secure the nation. The Identity Management System, in general, and Federated Identity Management System, in specific, should protect individual rights, provide enhanced privacy, and prevent fraud to lessen the risk of identity theft online.

A Trust Framework needs to be developed where the users, the service providers and other stakeholders can improve their use of online IdM systems. For achieving this, high level actions are needed that support the maintenance of governance, management and execution level activities to achieve the trusted Identity Management System. The government bodies, in collaboration with entities like individuals, businesses, non-profit organizations and lawyers, must lead the way to improve how identities are trusted and used in cyberspace.

REFERENCES

[1] Action Plan on e-signatures and e-identification to facilitate the provision of cross border public services in the Single Market," COM (2008) 798 final (28 November 2008); available at http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0798:FIN:EN:PDF

[2] Organization for Economic Co-operation and Development (OECD) Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication, June 2007, at p. 7; available at http://www.oecd.org/dataoecd/32/45/38921342.pdf.

[3] Australian National Audit Office, Attorney–General's Department Arrangements for the National Identity Security Strategy, ANAO Audit Report No.29 2009–10, April 21, 2010; available at www.anao.gov.au/uploads/documents/2009-2010_Audit_Report_29.pdf.

[4] Treasury Board of Canada Secretariat, Directive on Identity Management, July 1, 2009; available at www.tbssct.gc.ca/pol/doc-ng.aspx?section=text&id=16577.

[5] Commission of the European Communities, Action Plan on e-signatures and e-identification to facilitate the provision of crossborder public services in the Single Market, COM(2008) 798 final, November 28, 2008;available at http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=197692

[6] OECD, "The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers", OECD Digital Economy Papers, No. 160, June 11, 2009; available at www.oecd.org/dataoecd/55/48/43091476.pdf

[7] Scottish Government, Privacy and Public Confidence in Scottish Public Services: Draft Identity Management and Privacy Principles, August 31, 2009; available at www.scotland.gov.uk/Publications/2009/08/PrinciplesConsultation

[8] "National Strategy for Trusted Identities in Cyberspace," (Draft, June 25, 2010), at p. 1; available at http://www.dhs.gov/xlibrary/assets/ns_tic.pdf

[9] "The New Federated Privacy Impact Assessment (F-PIA):Building Privacy and Trust-enabled Federation" (January, 2009), http://www.ipc.on.ca/images/Resources/F-PIA_2.pdf

[10] The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers, DSTI/ICCP/REG (2008)10/FINAL, (June 11, 2009), available at http://www.oecd.org/dataoecd/55/48/43091476.pdf.

[11] "Identity Management Task Force Report 2008," (September 2008) available at http://www.ostp.gov/galleries/NSTC%20Reports/IdMReport%20Final.pdf

[12] "Certification Authority Liability Analysis" ; available at http://www.wildman.com/resources/articles-pdf/ca-liability-analysis.pdf

[13] Liberty Alliance specifications available at http://www.projectliberty.org/liberty/specifications 1

[14] "Surveillance or Security? The Risks Posed by New Wiretapping Technologies" Susan Landau, MIT Press, 2010.

[15] http://kantarainitiative.org/confluence/display/TFMMWG/Trust+Framework+Meta+Model

[16] "Use Cases for Identity Management on Internet" by, Robin McKenzie, Malcolm Crompton, Collin Wallis published in IEEE SECURITY & PRIVACY, March /April 2008, computer.org/security

AUTHOR'S PROFILE

Aparajita Pandey is an Assistant Professor at B.I.T.(MESRA), Jaipur Campus. Her qualifications include B.E.(EEE) ,MBA. She is also a MCSE and has a diploma in Cyber law. She has teaching experience of about 10 years in the areas of Circuit Analysis, Data Communication and Computer Networks. She is also a member of IAENG and ISOC. Her research interests include Online Identity Management, Internet Trust, Privacy and Network Security.

Dr. Jatinderkumar R. Saini is Ph.D. from Veer Narmad South Gujarat University, Surat, Gujarat, India. He secured first rank in all three years of MCA in college and has been awarded gold medals for this. He is also a recipient of silver medal for B.Sc. (Computer Science). He is an IBM Certified Data Associate- DB2 as well as IBM certified Associate Developer- RAD. He has presented 14 papers in international and national conferences supported by agencies like IEEE, AICTE, IETE, ISTE, INNS etc. One of his papers has also won the 'Best Paper Award'. 9 of his papers have been accepted for publication at international level and 13 papers have been accepted for national level publication. He is a chairman of many academic committees. He is also a member of numerous nation and international professional bodies and scientific research academies and organizations.