In proceedings of the International Conference on Informatics, Electronics & Vision (ICIEV), 2012

Identity Federations: A New Perspective for Bangladesh

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

Mohammad Jabed Morshed Chowdhury
Chief Technical Officer, Centre For Technology Development, Dhaka, Bangladesh
E-mail: jabedmorshed@gmail.com

Md. Moniruzzaman
Department of Computer Science, University of Calgary, Canada
E-mail: mmoniruz@ucalgary.ca

Farida Chowdhury
Department of Computing Science and Mathematics, University of Stirling, Scotland
E-mail: fch@cs.stir.ac.uk

Abstract— **With a view to provide more effective, enhanced and accessible services to their citizens, Governments around the globe have started different web services under the initiative of e-Government. Many such services extensively utilise the Federated Identity framework due to its huge number of benefits. This paper analyses how different e-initiatives in Bangladesh can take advantage of this technology by illustrating use-cases in two different domains. As the online service and the e-Governance paradigm in Bangladesh are relatively new and evolving rapidly, we believe that this is the high-time to consider the benefits this technology can bring for the Government as well as the citizen.**

Keywords- Identity fedaration, authentication, security

I. INTRODUCTION

Currently there are literally thousands of websites around the world providing a plethora of different services via the Internet. Originally, the protocols for digital communication were mainly designed to exchange information efficiently and reliably and the web and web-based services were not foreseen in its current form. At that budding stage, the identities of communicating parties could be assumed, and there was no need to verify it formally. It led to the omission of Identity Layer which could be used for formal verification of Identity [1]. As the web and web-based services started to evolve, verification of identity became a crucial part as Service Providers (SP, in short; the administrative body that offers and provides any service) need to identify users, to provide correct services and only to the authorised users. To adjust the situation, the process of authentication was subsequently added to verify the correctness of claimed identities. The authentication process requires users to register to generate or retrieve required identities which are usually accompanied with another or security token known as the credential. As the number of web-services as well as the user-base was expanding rapidly, more and more identities and credentials were issued, and soon their management became challenging, both for service providers and for users. Identity Management (IdM, in short) was introduced by the industry to facilitate online management of user identities which resulted in various different identity management systems.

Initially, these systems were not are interoperable, meaning identity authentication performed in one system was not recognised by others. However, as the landscape for web and web-based services started to change, novel business scenarios (e.g. B2B or Business to Business) started to emerge which required collaborations between business partners. To facilitate such collaborations, a novel Identity Management, called Identity Federation (also known as Federated Identities or Federation of Identities), was introduced which enabled organizations to provide services across their own borders by transferring authenticated identities among their trusted partners and collaborators. This paper aims to bring this exciting technology into the attention of different stakeholders involved in providing different web-enabled services in Bangladesh by providing a soft introduction to the technology at first and then illustrating how this technology can be fitted into the web-service landscape in Bangladesh.

With that said, the rest of the paper is organised as follows. Section 2 outlines the background concepts related to Identity Management and Identity Federation along with its many advantages. Section 3, then, discuses a few use-cases on two different domains, the Government and Higher Educational Institutes, to highlight the prospect of Identity Federation in Bangladesh. We discuss the security and privacy issues in Federated services in Section 4, describe a few related works in Section 5, outline a few technical challenges to implement this technology in Bangladesh in Section 6 and we conclude in Section 7.

II. PRELIMINARIES

Identity Management: Formally, Identity Management consists of technologies and policies for representing and recognizing entities using digital identifier within a specific context [2], [3]. Microsoft's .NET Passport [4], Liberty Alliance's Architecture[5], Shibboleth [6], OpenID [7], Microsoft's Card Space [8], Eclipse's Higgins [9], SourceID [10], DotGNU Virtual Identities [11], etc. are the examples of different Identity Management systems.

Service Provider: A service provider (SP, in short) usually provides service to the clients or to the other service providers. Examples include mobile phone operators, different web

service providers, etc. [12]. In its simplest form, a service provider may also include an identity provider (see below).

Identity Provider: An identity provider (IdP in short) provides digital identity to entities to enable them to receive service from a service provider. In its general form, it includes a credential provider.

Client/User: A client/user receives services from a service provider. To receive the service, the client usually needs to supply a digital identifier and a related credential to be authenticated as the valid user of that service.

Identity Domain: An identity domain is the virtual boundary, context or environment in which a digital identifier is valid, that is, it can be used to uniquely identify an entity.

Single Sign On (SSO): Single Sign On is the capability that allows users to log-in in one system and then access other related but autonomous systems without further log-ins. A good example is the Google Single Sign On service which allows users to log in a Google service, e.g., Gmail, and then allows them to access other Google services such as Calendar, Documents, YouTube, Blogs and so on.

Identity Federation: A federation with respect to the Identity Management is a business model in which a group of two or more trusted partners legally bind themselves with a business and technical contract. It allows a user to access restricted resources seamlessly and securely from other partners. The system that manages Identity Federation is commonly known as Federated Identity Management (FIM) System. Using a FIM System, users can authenticate themselves in one identity domain and receive personalised services across multiple domains without any further authentication [13]. A federation can be formed within a single identity domain that consists of only one IdP and more than one SP with each SP being a separate autonomous organisation. It can also be formed among several identity domains where each domain may consist of several IdPs and SPs. The issue of trust is a fundamental concept in FIM as different autonomous bodies need to trust each other inside the federation and thus form the so-called Circle of Trust (CoT).

FIM offers a good number of benefits to both different organisations and their users [13], [14]. It provides the advantage of separation of duties between the SP and IdP, scalability for SPs, generating revenue for IdP through their authentication services to the SP, standard based approach with improved security and privacy and easy integration of new stakeholders by expanding the circle of trust. For users, it offers SSO with security and privacy and alleviating the need to remember many user-ids and passwords for accessing different services.

III. BANGLADESH PERSPECTIVES

Bangladesh is still at its infancy in providing web based services to its citizens in comparison to the developed countries. The diversity and the huge range of web-based services one experiences in the developed countries are just not present yet. This is also reflected in many web traffic reports. According to these reports, the top visited websites in Bangladesh include the online version of the popular daily newspapers, several Bengali blogging websites, Bengali magazines, Bangladeshi job portals, etc. [15], [16]. Bangladeshi Government under the e-Government initiative is committed to establish a solid e-infrastructure throughout the country so that its citizens can get necessary services through websites from their home. Currently, the focal point of such services is the National Web Portal of Bangladesh [17] which enlists a wide range of e-initiatives from the Government of Bangladesh. Unfortunately, none of them are among the top visited websites according to the web traffic report [15], [16]. The reason could be that those services are still not matured enough to attract people's attention and therefore they do not feel the necessity to visit there. There is no doubt that more people will use these services if their range and quality increase. The same thing can be said regarding the quality of web services that can be found in the higher educational institutes in Bangladesh. There are currently 30 public, 54 private universities, two international and two special universities that are functional as of July 2011 [18].

Many of these websites are below average in terms of quality and merely provide any useful services other than providing some basic information or email facility to faculties and vary rarely to the students. However, they are evolving fast and most of them may reach up to a standard very soon. As both the e-Government initiatives and the web services in Higher education sector are evolving, we would like to take the opportunity to investigate how identity federation can be used to improve the underlying infrastructure as well as to offer better services. We outline the advantages in the following case studies.

A. Case Study 1: e-Governance in Bangladesh

In today's world, Governments and business organizations around the world heavily use Internet for increasing their efficiency. In such online environments, it is essential to share sensitive personal and business information securely among different government offices as well as with citizens and different business partners. An FIM infrastructure can be the ideal choice to share such information securely across organisational boundaries which would reduce administrative and infrastructure cost while increasing efficiency with enhanced security. In the following, we explain how Bangladeshi government can use the Federated IdM to get these advantages [13].

Government to citizen: Centre to any IdM system is the Identity that determines who a person is online and a Government is the first authority to create an official identity for a citizen in the form of a birth certificate. Then the government keeps providing different Identity documents such National ID card, Passport, Driving License, Tax Identification Number, Marriage certificate, Death certificate, so on and so forth. All these ID documents are provided by different governmental organisations. The traditional non-federated e-services would require a citizen to visit different websites to receive respective services and need to manage different credentials which soon would become a problem for a citizen. Moreover, many of such services would warrant for enhanced security and privacy. As mentioned earlier, the

Govt. of Bangladesh has undertaken many e-initiatives to provide better services towards her citizen as well as to reduce the difficulties many people face to avail these services in the current setting. Unfortunately, the need for security and privacy in these initiatives is simply overlooked in many cases. One of the prime examples is the Result publishing website by the Intermediate and Secondary Education Boards, Bangladesh (http://www.educationboardresults.gov. bd/) that is being used actively to publish the result of different public examinations such as JSC, SSC, HSC, Alim, Dakhil, etc. This is an excellent service that allows students to receive their exam results as soon as published which significantly reduces the complexities as well as troubles one had to go through to collect his/her results previously. However, the main focus of this website is just to publish the result ignoring the need for security and privacy. To illustrate the devastating as well as negative impacts such lacking could have, let us consider the following two scenarios:

i) The service interface is very simple – anyone can view the result of anyone by entering the correct Roll number, selecting other appropriate parameters such as the name, Year and Board of the exam. This information submitted into the server which, presumably, queries the database using the submitted parameters and upon finding the required information send the result which are then displayed in the browser. However, the website and the service do not use any transport layer security such as SSL (Secure Socket Layer) or TLS (Transport Layer Security) and thus unable to satisfy two (Confidentiality and Integrity) out of three (Availability being the third one) key components of Information Security [19]. Lack of Confidentiality will allow any attacker to look at the information while they are en-route from the server to the client and lack of Integrity will allow any attacker to alter the contents while they are en-route such that falsified result may appear on the client browser, e. g. the result of a student will show Pass where he/she eventually has failed and vice-versa. Such an attack cannot change any result, however, stored in the database and submitting the query from another network will eventually show the correct result. Nevertheless, such scenario could be particularly dangerous as well as intimidating considering the impact it can have over the victim. We analyse these issues in details in Section 5.
ii) Another issue is of privacy. The service being very open will allow anyone to view anyone's result. After submitting a random value as a Roll number, we have been able to retrieve someone's results fairly easily. It also includes private information such as Date of Birth, Exam Result, etc. which are quite private in nature are open to public. These sorts of information should only be accessible by authorised personnel. This clearly can invade someone's privacy, even if he or she may not be aware of the situation. We analyse the privacy in details in Section 5.

Such lack of security and privacy issue can be greatly taken care of and other complexities can be reduced significantly using any federated approach. This is outlined in the following use-cases.

i) Assuming, the Government of Bangladesh has established Federated Identity services for their citizens linking different governmental services together. The focal point of such services is the National Personal Portal of a citizen. The infrastructure could be based on SAML (Security Assertion Markup Language, protocol to enable Identity Federation) using the SAML compliant IdP and SP such as Shibboleth, SimpleSAMLphp, ZXID, OpenSSO, Lasso, etc. [20]. Because of its php interface let us assume that the SPs are using SimpleSAMLphp to provide SAML-enabled services. Use-cases based on other SAML implementations can be easily accommodated into our use-cases without any change or with a very few changes in the following steps.
ii) Mr. Rahim is a citizen of Bangladesh. He is provided with the National ID card. For the sake of this example, we assume the ID no. in the card acts as the user-id for any citizen. Also for brevity, we are assuming a password based credential; however, it can be anything such as smart card, hardware token, digital certificate, etc. for enhanced security. He needs to avail some governmental services and so he visits the National Personal Portal.
iii) Before he can access any service, he needs to authenticate himself. The SAML interface of the portal checks if there is a security context signifying Mr. Rahim is already authenticated. Assuming not, the portal will redirect the user to the SSO services of the central Identity Provider.
iv) The SSO service checks if there is any security context meaning the user is already authenticated. Assuming no previous authentication, it displays the authentication page to the user.
v) Mr. Rahim types in his ID no and the related password and hits the enter key. Being a part of the SAML federation, all communicates are secured with industry standard security such as Web PKI using HTTPS protocol which ensures the submitted user-id and credential will not be transferred in plain text.
vi) The SSO service at the IdP validates authentication and if successful, redirects him to the assertion consuming service at the National Portal with a security context embedded inside the SAML assertion.
vii) The National Portal displays the Homepage to Mr. Rahim.
viii) Mr. Rahim has changed his house since last time he visited the portal. Therefore, he wants to change his registered address. He chooses the National Population Registry link. Being a different service provider, he is forwarded to the Registry service.
ix) Scenarios of step iii will take place.
x) The SSO service at the IdP will find that the user is already authenticated and thus no need for authentication and it redirects the user to the assertion consuming service at the Registry service with a security context

embedded inside the SAML assertion.

xi) Upon receiving a successful security context, the Registry service displays the page where he can change his address and saves it.

xii) Upon completing the task, he is redirected back to the National Portal. Now he wants to return his annual income tax and so chooses the tax return link.

xiii) This takes him to the National revenue service and the previously mentioned flows take place.

xiv) Finishing all his tasks, Mr. Rahim log out from the National Portal. He is very pleased with the federated services as he needs not visit different websites and logs in several times with different credentials. It has made his life simple.

Intra-Government use-case: The previous use-case can be used to exemplify an Intra-Government use-case. Different vital information sometime needs to be shared among several organisational boundaries inside Government, for example among different ministries. As before, the traditional identity systems would require one to have accounts at different organisations to access resources located in different autonomous organisations. Following the scenarios from the previous use-case, a federated approach would be simple and easy to use yet secure and well-organised. We're not providing any use-case for these scenarios to keep the length of the paper reasonable.

Government to business: Likewise, the Government has to offer different services to other business organisations and they in return need to provide different information at different times. Company registration, license maintenance, VAT declarations – all these services require a business enterprise to contact at different Government organisations. Like before, a federated approach could be ideal for such scenarios and we are omitting for these scenarios to shorten the length of the paper.

B. Case Study 2: Higher Educational Institutes in Bangladesh

e-Service in Higher Education sector is extremely important. This allows users (students, teachers, researchers and administrative authorities) to access the respective services from anywhere via Internet. For students, example of such services could be the respective Student Management System that will allow them to update and maintain their student data as well as access library to order new resources and renew their borrowed ones. For teachers, such service could allow them administer course related data and such examples could be given for other stakeholders. Administratively, such institutions consist of different departments each being autonomous yet collaborative in different contexts. As mentioned earlier, Identity Federation offers a lot of advantages in such scenarios. Not to mention, many information passing between these bodies are highly sensitive thereby requiring a system with enhanced security. We will present two use-cases to illustrate the advantages in Intra-University and Inter-University settings.

Intra-University:

i) Rahim is a student of the ABC University which has enabled Federated services among its different administrative and academic organisations.

ii) Rahim wants to accomplish a few tasks from his home. The focal point of the services offered to the students is the Student Portal System. Rahim visits the Student Portal System.

iii) Like before, the Student Portal System will check if he already has a session. If yes, it skips steps iv and v.

iv) Rahim is redirected to the central University IdP where he has to authenticate himself.

v) Upon successful authentication, he is again redirected to the portal with his identity information.

vi) Having authenticated himself, he lands on the homepage of the portal.

vii) There are links for different services and he, at first, wishes the check his email and so clicks the link for emails.

viii) He is forwarded to the email service which redirects him to the IdP again (assuming there is no previous session with the email service).

ix) The IdP finds the user is already authenticated and so redirects him again to the email service with the identity information.

x) He can now read, send or do whatever related to the email services.

xi) Once he completes using the email service, he wants to visit the library service to renew his book loan.

xii) He clicks the library link and the usual flows take place.

xiii) After completing the task at the library website, Rahim wants to order his transcripts and so he clicks the Transcript link that will take him the Examination Control Office which is responsible to provide this service and again the usual flows take place.

xiv) Once he is done, he logs out.

A Federated approach has saved time and hassle for him by allowing him to avail different services by logging in just once. In traditional setting, he would have to log in at least four different places.

Inter-University: Collaboration among different universities is a key feature in western universities. During collaborations, researchers need to share different resources among themselves securely. Federations can be used to securely share such resources across the universities that will allow researchers from one university to access resources located at another university using the credential of the first university. Not only for a joint research program, federations can be used by any related individual of a university to access a resources at other universities with minimum effort.

IV. SECURITY & PRIVACY ISSUES

Major concerns in Federated services are different security and privacy issues. Security requirements refer to the mechanisms that are utilised to establish and retain security of the user during the lifetime of the relationship between a user and the corresponding SP. Privacy requirements refer to the conditions that an organisation must follow to protect and preserve confidential user data from unauthorised access. In traditional web-based services where each SP has its own

identity and security domain, security requirements for that respective service are regulated by that SP. For example, the SP determines solely if it needs a specific security infrastructure (e.g. Web PKI) for its services. Similarly, Privacy is of little concern in such settings as privacy requirements are governed solely by that respective organisation and any breach of user-privacy is more likely to be confined there within. However, when different identity and security domains are involved and the user data are to cross those domains, it is very important to establish a common yet strong security and privacy model across all domains to ensure that a relatively weaker model in any one domain cannot undermine the security and privacy in other domains. Generally, Federated Systems are relatively based on a strong security model. Unfortunately, the privacy model is relatively week and tends to vary from one service to another as different services have different privacy requirements. In this section we will analyse different security and privacy issues in SAML based Federated Systems.

A. Security Requirements

The core requirements that guarantee the security of any transmitted user data in an information system are: Confidentiality, Integrity, Authenticity, Non-repudiation and Availability [19]. Confidentiality ensures that the user data is disclosed only to the intended and authorised party. Integrity guards against the malicious and intentional modification of the user data during transmission. Authenticity ensures that parties involved in a transaction can prove what they claim to be and the data is generated from the original source. Non-repudiation guarantees that once a party in a transaction commits into a transaction it cannot deny it. SAML utilises the PKI with SSL/TLS protocol and digital certificates to ensure Confidentiality, Integrity, Authenticity and Non-repudiation where each assertion in SAML is encrypted and digitally signed to meet these requirements. To enable this, each service provider has to deploy Web PKI using digital certificates to be a part of the SAML Federation. The fifth security requirement Availability is to ensure that an entity can provide services when required. However, ensuring service availability of each entity (SP and IdP) in the federation are business decisions regulated by each organisation. That is why there is not any concrete requirement specified in the SAML to ensure such level of availability. There are many methods to ensure availability based on reliability theory and the organisation has to choose their own to reflect their business policy.

B. Privacy Requirements

Privacy is a complex issue that changes over time and tends to vary considerably from one country to another. However, the core requirements here are to consider the usage of Anonymous/Pseudonymous Identifier during a transaction and to control identity linkability across different organisations. In Federated settings, users provide their identifiers to the IdP and the IdP generates/releases an anonymous (or a pseudonymous) identifier inside the assertion for the SP. The ideal way to preserve the user-privacy is to deploy a per-site pseudonymous identifier so that the IdP will generate a pseudonymous identifier for each specific SP. In the context of this paper, while providing Government to citizen services, it may not be very relevant or even necessary to use pseudonymous identifiers to access the services. However, in Government-to-business cases, it must preserve the user-privacy in those organisations as there is no guarantee a group of organisations may not act maliciously. SAML supports the generation and release of per-site pseudonymous identifier.

V. RELATED WORK

There are many ever-growing examples of Identity Federation, both in the Government sector and the higher education sector, around the world. Some countries have federated web services like DigiD in the Netherlands [21], E-government in New Zealand under e-GIF Standard [22], while others have a central SSO enabled portal such as Government Gateway in UK [23], Danish IT Citizen Portal [24], GovHK and MyGovHK in Hong Kong [25], My eID in Belgium [26], MyPage in Norway [27], Bürgerkarte in Austria [28], etc. There are ample examples of federation in education sector such as UK Access Management Federation for Education and Research [29], the SWITCH in Switzerland [30], Feide in Norway [31], CARSI in China [32], CAFe in Brazil [33], InCommon in USA [34], etc. And these numbers are growing very rapidly.

Sadly, e-Services are still at its budding stage in Bangladesh. We're just experiencing several initiatives in the Government to implement different services via Web. Identity federation can greatly improve these services. To the best out knowledge, we did not find any proposal or implementation regarding identity federation for e-Services in Bangladesh.

VI. DISCUSSIONS

A list of recommendations regarding e-Government in Bangladesh can be found in [35], [36]. We are enlisting a few of them below to exemplify the ways identity federations can be used to achieve and utilize them.

i) e-Government should be better integrated with civil service reform: To achieve this goal, it is essential to ensure civil service authorities are accountable, open and responsive and consequently each public service reaches the doorstep of every citizen. These criteria can only be met with e-Initiatives via the Internet. A Personal Portal could be used to combine every single public service and act as a single focal point to offer all services. Identity Federation is the key to accomplish such scenarios efficiently and securely.

ii) Infrastructure and Connectivity: It has been suggested to provide Broadband Internet access to Govt. offices down to Upazilla level, expand shared access in LGIs, post offices and schools and build a National data centre and National ID platform for e-services. Broadband access at the Upazilla level can ensure the required underlying infrastructure and federation can utilize it to provide shared accesses at root level via web-enabled services. National data centre can be the central database and act

as the central Identity Provider for the federation. National ID can be used as the core user-id with a suitable credential. A standard Web Public Key Infrastructure (PKI) needs to be integrated with these service to ensure security and privacy.

iii) Better coordination of e-Government strategy and planning: One of the core advantages of the federation is the better coordination among disparate organisations; therefore, federations can be used as a tool to achieve this.

iv) Security of authentication in e-Services can be improved with federated services. As this a single point of authentication, it will be relatively easier for the Government to ensure state of the art security measures for this infrastructure. In the same time, The Government should be very careful otherwise it will be a single point of failure.

v) This will pave the way to achieve interoperability between different e-Initiatives of the Government.

vi) This will also ease the life of the Government web service developers and maintenance staffs. As developers will be provided with standard authentication mechanisms, they do not have to bother about the authentication

vii) As the federation standard uses standard procedures, it will help or foster the standardization of other e-Service interfaces.

VII. CONCLUSIONS

In this paper we have briefly analysed the advantages of identity federation and how they can be used to simplify many aspects e-Services for every party involved. Security and privacy are deeply integrated into the federation standard which comes as an added benefit. Many countries around the world are adopting federated standards for their rich list of benefits. Government of Bangladesh can get the benefits by adopting the identity federation. However, considering the current level of e-Services, building a federation within Government organisations is a mammoth task. It requires insightful vision, rigorous planning, sufficient fund and above all the willingness to achieve them. On the other hand, the complexity and scale is much less for Higher Education institutes. Most universities are yet to build their own infrastructures for e-Services. The University Grant Commission can lay down a combined plan that the universities will utilize to build their infrastructures with the possibility for expansion to the federations. As the e-Service landscape of Bangladesh is just forming, we believe that this is the best time to envision the crucial role identity federations can play in e-Services and then plan and act accordingly.

REFERENCES

[1] Kim Cameron: The Laws of Identity. May 2005. http://www.identityblog.com/stories/2004/12/09/thelaws.html

[2] Md. Sadek Ferdous. Identity Management with Petname Systems. Master's thesis 2009. http://ntnu.diva-portal.org/smash/get/diva2:347842/FULLTEXT01

[3] Jøsang, A., Al Zomai, M., Suriadi, S.: Usability and privacy in identity management architectures. In: L. Brankovic, C. Steketee (eds.) Fifth Australasian Information Security Workshop (Privacy Enhancing Technologies) (AISW 2007), {CRPIT}, vol.68, pp. 143--152. ACS, Ballarat, Australia (2007).

[4] Microsoft .NET Passport. www.passport.net

[5] Liberty ID-FF Architecture Overview Version:1.2-errata-v1.0 http://www.projectliberty.org/liberty/content/download/318/2366/file/draft-liberty-idffarch-overview-1.2-errata-v1.0.pdf

[6] Shibboleth Project. Shibboleth Architecture Protocols and Profiles. Working Draft 05, 23 November, 2004. Internet2/MACE, 2004

[7] OpenID. http://openid.net/

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

[9] Higgins- Open Source Identity Framework. http://www.eclipse.org/higgins/index.php

[10] SourceID-Open Source Federated Identity Management. http://www.sourceid.org/

[11] DotGNU Virtual Identities. http://www.gnu.org/software/dotgnu/auth.html

[12] Wikipedia entry on service provider. Accessed on June 25, 2011. http://en.wikipedia.org/wiki/Service_provider

[13] Liberty Alliance Whitepaper: Benefits of Federated Identity to Government, March 7, 2004. http://projectliberty.org/liberty/content/download/388/2723/file/Liberty_Government_Business_Benefits.pdf

[14] David W Chadwick. Federated identity management: In A. Aldini, G. Barthe, and R. Gorrieri, editors, *FOSAD 2008/2009*, number 5705 in LNCS, pages 96-120. Springer-Verlag, Berlin, January 2009.

[15] Top Sites in Bangladesh by Alexa. Accessed on 08 July, 2011. http://www.alexa.com/topsites/countries/BD

[16] Top 20 popular Bangladeshi websites. Accessed on 08 July, 2011. http://banglacomputing.net/top20sites.php

[17] National Web Portal of Bangladesh. http://www.bangladesh.gov.bd/index.php?option=com_frontpage&Itemid=1

[18] List of Universities in University Grant Commission. Accessed on 08 July, 2011. www.ugc.gov.bd

[19] Wikipedia entry on Information Security. Accessed on June 25, 2011. http://en.wikipedia.org/wiki/Information_security

[20] SAML Open Source Initiatives. http://saml.xml.org/wiki/saml-open-source-implementations

[21] http://www.digid.nl/english/

[22] http://www.e.govt.nz/

[23] http://www.gateway.gov.uk/

[24] https://www.borger.dk/Sider/default.aspx

[25] http://www.gov.hk/en/residents/

[26] http://eid.belgium.be/

[27] http://www.norway.no/minside/

[28] http://www.buergerkarte.at/

[29] http://www.ukfederation.org.uk/

[30] http://www.switch.ch/aai/

[31] http://www.feide.no/

[32] http://shibboleth.edu.cn/

[33] http://wiki.rnp.br/pages/viewpage.action;jsessionid=B195EB224503DECD433A70C5A2DCB37E?pageId=41190088

[34] http://www.incommonfederation.org/

[35] Bangladesh Enterprise Institute (BEI) report: Realizing the Vision of Digital Bangladesh through e-Government. July 2010. www.bei-bd.org/downloadreports/view/48/download

[36] Report from the Prime Minister's office: Digital Bangladesh for Poverty Reduction and Good Governance, June 2010. https://docs.google.com/fileview?id=0B54YW0mcQI63OGU5ZjI1ZjQtZTc2Ni00MGE3LTk2NjgtNjU1YjMyNTYyNGE1&hl=en&pli=1