E-Government Trust Frameworks in the United States

Paper presented at the Symposium on
"Neither Public nor Private: Mixed Forms of Service Delivery around the Globe"
17-18 May 2012, Barcelona, Spain

Gilad L. Rosner
Ph.D. Candidate
University of Nottingham
School of Computer Science
psxgr@nottingham.ac.uk

Introduction

This paper describes empirical research on the public/private character of identity management systems used for E-Government in the United States. Little is written on this subject in academic literature, and the area is a site of active technical and policy evolution. This research – part of the author's broader doctoral work – contributes to the multidisciplinary domain of information policy, and is hopefully of use to scholars of public policy, identity management, and E-Government.

Governments around the world are in various stages of designing and deploying federated identity management (IDM) systems to enable citizen access to E-Government services. To comply with privacy law, governments must ensure that citizens are *authenticated* when accessing services that exchange personal data. This requires digital credentials be reliably bound to citizens, with a high degree of assurance that the attached identity has been appropriately validated. In countries that have no national citizen register, such as the US, hybrid public/private identity management systems are being built to address the need for strong authentication. These systems rely on organizations external to government to supply citizens with the means to access online services. A key challenge inherent in these systems is constructing a mechanism for governments without national registers to trust the validity of a credential. To overcome this, the US is applying a risk methodology based on the potential for harm in the case of an authentication error, and on 'Levels of Assurance' of the validity of an asserted identity. Private non-profit and for-profit actors as well as government agencies and advisory bodies are part of the evolving effort to enable online citizen access.

The research is based on a combination of methods: semi-structured interviews with 27 stakeholders carried out in 2011 and 2012, a literature review, an analysis of official documents and technical specifications, and observation at various industry and government conferences. Expert representatives in technical, legal, operational and policy-making roles were selected as interview subjects from federal agencies, non-profit and for-profit companies, law firms, privacy advocates and independent consultants.

E-Government

Electronic Government, or E-Government, is a broad term encompassing the use of electronic and internet technologies to deliver government services and increase citizen-government participation. One common trend is the transition of paper-based and in-person interactions to the World Wide Web, as well as the creation of new interactions that did not exist prior to the creation of electronic channels. In the US, there is a wide variety of online government services: license registrations and renewals, driving practice tests, health record searching, tax filing, traffic and weather conditions, road damage reporting, benefits eligibility pre-screening, disaster assistance information, court information, and consumer protection complaint forms (OMB, 2012; West, 2007). As E-Government began to grow in the US, a key supporting policy was enacted: the E-Government Act of 2002, passed "to improve the methods by which Government information, including information on the Internet, is organized, preserved, and made accessible to the public"(44 U.S.C. § 101 (a)). Every year, the Office of Management and Budget reports to the US Congress on the state of federal E-Government initiatives. As of 2011, there were over 5,600 public-facing government websites (.gov Reform Task Force, 2011).

Many meaningful interactions between citizens and government require an exchange of personal information. The United States, like many countries, has laws and policies that constrain the distribution of personal and sensitive information. The central policy that controls how federal agencies share personal information is the Privacy Act of 1974, which states:

> *No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except*

> *pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains...*(5 U.S.C. § 552a (b))

To comply with this and related policies, agencies must know with whom they are interacting. Otherwise, they could not know definitively if someone is authorized to see a subject's personal information. When conducting transactions in person, this issue is usually addressed by the relevant party showing an official form of identification; often, in the US, a driver's license. Moving information exchanges to the Web complicates this – there is no reliable method to authenticate a person with traditional forms of official identification over the internet. A chief value of identity documents like driver's licenses, state-issued ID cards and passports is the difficulty in counterfeiting them and the ability for an agent to compare the embedded photo to the person presenting it. Both of these security features are nullified by electronic automated transactions conducted at a distance. As such, it is difficult to positively identity citizens in online transactions on a national scale. The US is not alone in facing this dilemma – many countries wishing to move government services to the Web are seeking create new ways to verify the identity of citizens with whom they interact in order to take full advantage of the productivity gains, cost savings and reach that Electronic Government offers.

Towards Trust Frameworks

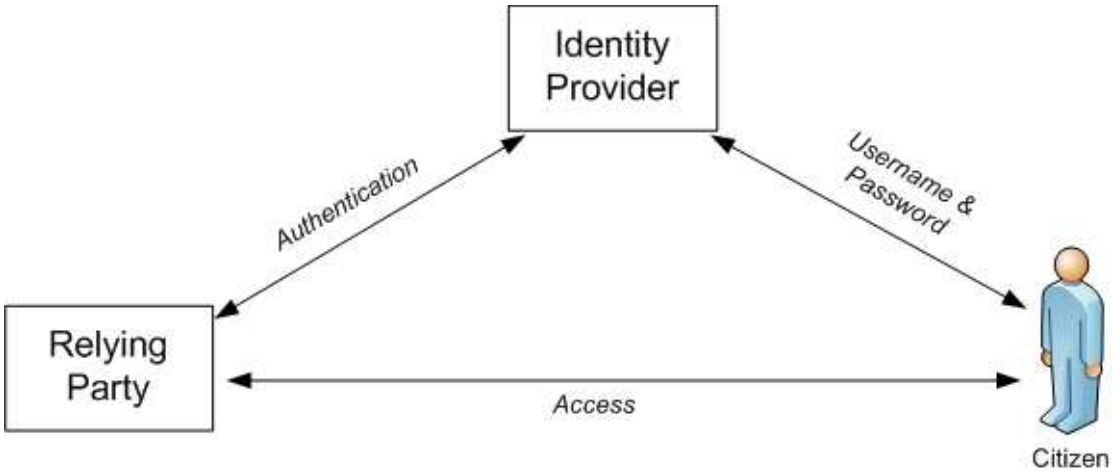
The United States has neither a national citizen register nor a requirement for its citizens to register themselves locally[1] – registration, in the form of birth certificates, occurs at the state level. There is no single national agency that is fully authoritative on the identities of the American populace. The Social Security Administration is purportedly the most authoritative and is the most suitable choice to act as a citizen identity authority, but it has declined this role in the past because of cost, complexity and politics, and there is no evidence that this will change. Moreover, there is a strong antipathy towards the idea of a national ID amongst the polity. It is characterized as a privacy invasion, dangerous and illiberal, with portents of totalitarianism by granting

[1] Male citizens must register themselves for potential conscription within 30 days of their 18th birthday as required by the Selective Service System. Social Security numbers are required in order to legally work in the US.

too much power to the federal government (Etzioni, 1999; ACLU, n.d.). This presents a challenge to the development of online credentials that can reliably identify citizens.

In the absence of a citizen registry and the political impossibility of building an identity service specific to E-Government authentication, the US decided to rely on credentials created by organizations outside the federal government. In the early 2000s, the federal government had begun a number of initiatives to build frameworks for federal entities to accept identity credentials from private financial institutions. Also, the government recognized that citizen credentials - digital identities - were organically appearing in commercial and academic domains: in online services such as Yahoo and Google, in electronic banking, and the wide proliferation of university logins. Members of the Government Services Administration, an independent agency with broad responsibility to support federal operations, envisioned an architecture of multiple external private organizations providing reusable credentials to citizens, and multiple separate federal agencies being able to 'consume' them. The general term for this arrangement is *federated identity.* The external credential issuer is known as the Identity Provider, or IDP, and the agencies that consume the credential are Relying Parties[2], or RPs - they rely on the identity assertion[3] of the IDP.

Fig. 1. Federated identity model.



Federated identity is an evolutionary change in credentialing on the Web. In order to personalize user experiences, websites needed to know when the same person was

[2] Some literature refers to these as Credential Service Providers (CSPs) and Service Providers (SPs).
[3] The term 'identity assertion' is used in the sense of a claim: a person or entity on her or his behalf asserts that the person is a specific, unique identity.

returning to the site. Traditionally, a website would enroll each person wishing to access it – a news site would supply one login[4], a bank another, a game site another, and on and on. As a result, over the years, users have accumulated a plethora of passwords[5] that are either difficult to remember, or are very simple, rendering them insecure. Where sensitive data is involved, this creates the potential for fraud. In the case of government agencies, it was understood that each agency supplying a different credential to citizens was both inefficient and undesirable. Not only would there be replicated efforts, but also inconsistency and a deepening of the password problem. In response, governments around the world, such as Austria, Germany, Canada, the UK, and Estonia, are all in various stages of building federated identity systems for online access to government services. These systems rely on the concept of a *single sign-on*: one credential with one password[6] used on a multiplicity of websites. By federating identity this way, all efforts to enroll citizens in the credentials can be carried out by a single group of issuers, and agencies can instead focus their efforts on the content of E-Government rather than citizen authentication.

In countries that have national registers, such as Austria, the data needed to create online credentials originate with the local and national government. That is, the Austrian government is authoritative on biographic and demographic data about its citizens (United Nations, 2005). The rules and activities required to enact a secure 'identity supply chain' – ensuring that credential production and subsequent binding to citizens were performed correctly– are controlled by the state. As such, there is inherent confidence in the procedures and the data. When an Austrian citizen presents her or his credential to an online government service, the content of that identity assertion and any attributes[7] therein can be assumed to be authentic and accurate. In the US plan to accept external credentials, the data and procedures that create them originate from a variety of *private* sources. By default, the data is not 'official', in the sense of a state-issued form of identity. How then can the government trust the digital identity? Official state forms of identity like driver's licenses or passports are created according to government standards and security procedures - the government thereby

[4] 'Login' and 'credential' for the purposes of this paper are interchangeable.
[5] See, for example, Florêncio, D. & Herley, C. (2007) *A Large-Scale Study of Web Password Habits*, Microsoft Research, available at https://research.microsoft.com/apps/pubs/?id=74164
[6] Sometimes augmented with a 'second factor' of authentication, such as an additional PIN code or a one-time password sent to a citizen's mobile phone.
[7] E.g., date of birth, address, healthcare identification number, etc.

trusts its own identity documents. When those procedures and data originate in private organizations, each with its own rules, needs, processes and security methods, the resultant identity documents – in this case, online credentials – become non-standardized, and their authenticity and security characteristics cannot be easily judged. To accept credentials generated by entities outside the government and still ensure that personal information is shared only with authorized parties, agencies needed a methodology to allow them to judge whether a credential was authentic and appropriately bound to a citizen, that the processes to validate the citizen's identity were sound and reliable, and that the credential provider complied with federal policies for exchanging personal information with the government.

In 2003, the Office of Management and Budget (OMB), the federal agency responsible for enacting executive policy, ordered all executive agencies to assess themselves as to the degree and likelihood of harm that would result from loss of or unauthorized access to personal data in their possession. This was done as part of their responsibilities to operationalize the E-Government Act and the earlier Government Paperwork Elimination Act of 1998. OMB detailed six categories of harm and impact that agencies were to consider in their assessment of risks from an authentication error:

- inconvenience, distress, or damage to standing or reputation
- financial loss or agency liability
- harm to agency programs or public interests
- unauthorized release of sensitive information
- personal safety
- civil or criminal violations

The potential impact values for these categories are Low, Medium and High[8]. OMB's risk methodology aligns the harm impact values with 'Levels of Assurance' (LoA) in an asserted identity.

[8] See OMB M-04-04 Sec. 2.2 for details of the application of each impact value to each category of harm.

Fig. 2. Impact category / Level of Assurance Matrix. Source: OMB M-04-04.

	Assurance Level Impact Profiles			
Potential Impact Categories for Authentication Errors	**1**	**2**	**3**	**4**
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

The Levels of Assurance are defined as follows: "Each assurance level describes the agency's degree of certainty that the user has presented an identifier (a credential in this context) that refers to his or her identity. In this context, assurance is defined as 1) the degree of confidence in the *vetting process* used to establish the identity of the individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued" (OMB M-04-04, pp. 4, orig. emphasis). The levels are:

- Level 1: Little or no confidence in the asserted identity's validity
- Level 2: Some confidence in the asserted identity's validity
- Level 3: High confidence in the asserted identity's validity
- Level 4: Very high confidence in the asserted identity's validity

OMB's methodology standardized agencies' policies regarding confidence in external credentials, but allowed each to make its own determinations about the right mix of data sensitivity, potential harm from loss or unauthorized access, credential enrollment reliability and security model. Once an agency concluded its assessment, it was to select technology appropriate to the Level of Assurance as specified by NIST, the National Institute of Standards and Technology. NIST's Special Publication 800-63 details security token[9] types, token and credential management system types, authentication protocols, cryptography standards, and attack types to be defended against. As the consequences from an authentication error increases, so do the Levels

[9] A token is the 'carrier' for a credential that a user possesses, like a password or a cryptographic module.

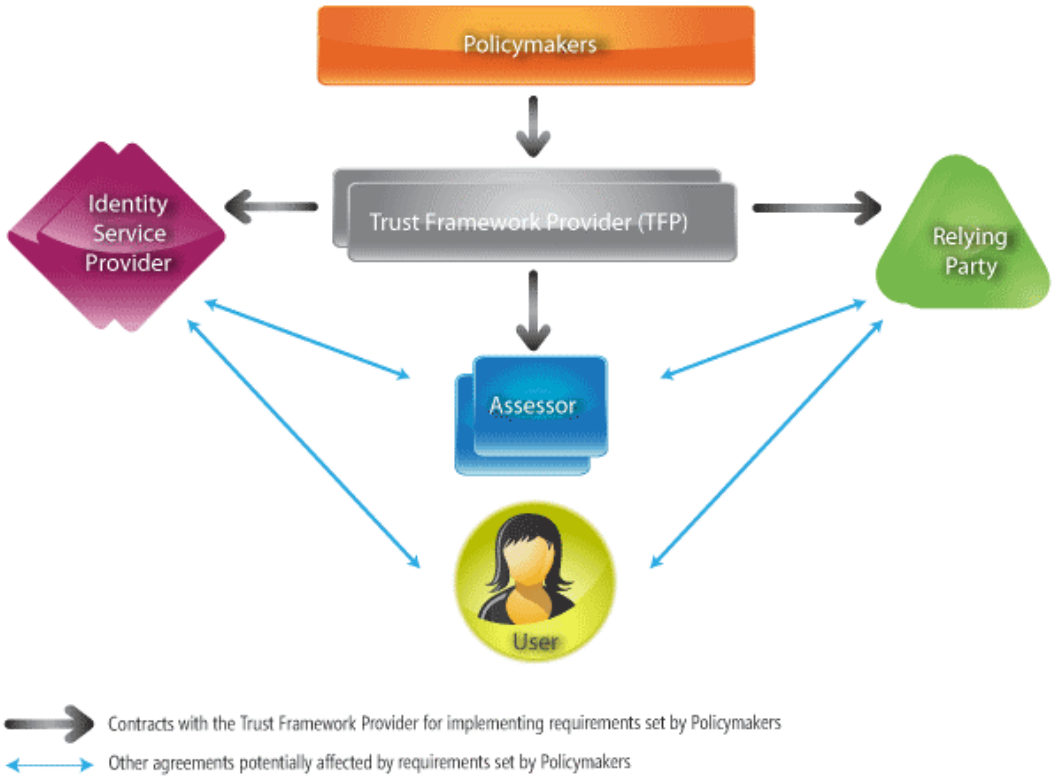
of Assurance, as well as the required security strength of the identity management system.

SP-800-63 also describes identity proofing requirements for credential issuers. Separated into ‘in-person’ and ‘remote’ applications for a credential, the NIST document specifies the types of existing identity proofs an applicant (e.g., a citizen) must provide to the credential issuer to validate his or her identity, the required method of validation, and any further actions the issuer must take in order to complete the identity assurance. For example, at LoA 3, in a remote application for a credential, an applicant must supply a government-issued ID number, such as a driver’s license or passport number, and a financial or utility account number, such as a checking account number, a water bill account number, or a credit card number. The credential issuer verifies the applicant’s identity “through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, [date of birth], address and other personal information in records are consistent with the application and sufficient to identify a unique individual” (NIST SP-800-63, pp. 34). Finally, the issuer either confirms the applicant’s address by sending information through the mail, or calls the applicant on the phone and “records the [a]pplicant’s voice or [uses] alternative means that establish an equivalent level of non-repudiation” (Ibid.).

In 2008, the federal CIO Council, comprised of the Chief Information Officers of all of the cabinet-level agencies and armed services, formed subcommittees to recommend policies for security and identity management initiatives relating to federal IT systems. One of these, the Federal Identity, Credential, and Access Management subcommittee (FICAM), was charged with producing the policies and procedures that would enable potential suppliers to meet government standards and needs for citizen digital identities. This meant building a framework to allow would-be IDPs to conform to the OMB Levels of Assurance methodology. FICAM was also responsible for ensuring technical interoperability between IDPs and RPs; government agencies would be able to adopt FICAM's technical standards rather than research and construct their own. FICAM also created a set of privacy and operational requirements for suppliers to interact with federal systems and citizen data. However, given the desire for a plurality of IDPs, FICAM did not wish to be responsible for

assessing and approving all of the potential suppliers, as this was considered burdensome. Instead, it devised a way to insert an intermediary between itself and potential credential issuers. The intermediary, known as a *trust framework provider*, or TFP, would shoulder the burden of certifying suppliers to a given Level of Assurance.

Fig. 3. A trust framework. Source: http://openidentityexchange.org/what-is-a-trust-framework



FICAM would give all of its policy and technical requirements to the TFP, who would transform those requirements into a form that could be assessed against. The TFP would accredit independent assessors who would evaluate potential suppliers against the assessment criteria. Should a supplier meet all of the requirements, it would be given a 'trustmark' in the name of the TFP; a supplier would become 'LoA *n* certified', where *n* is 1 to 4. This way, federal agencies that had assessed themselves according to the OMB methodology and decided that LoA 3, for example, was required for a particular online service, could enter into lightweight business negotiations with an LoA 3 certified identity provider and consume its credentials confident that the provider met federal requirements.

The Chief Information Officer of the US instructed FICAM to consider accepting an identity technology known as OpenID – it was thought there were millions of OpenID credentials in consumer use at the time. FICAM and the CIO approached the OpenID Foundation, the steward of OpenID protocols and technologies, and asked if they would consider becoming a trust framework provider. Seeing this as beyond their remit, they declined, but a subsidiary organization was spawned to take on the task – the Open Identity Exchange (OIX). OIX would ultimately be joined by three other TFP's: the InCommon Federation, who manages the federated identity system known as Shibboleth; Kantara, an evolution of a group called the Liberty Alliance, which was closely linked to the genesis of the SAML identity assertion protocol[10]; and Safe/BioPharma, an association of biopharmaceuticals and healthcare communities. Though different in structure, constituency and purpose, these organizations were intended to enable their members, potential credential suppliers, to technically interoperate with federal agency IDM systems, and meet operational and privacy requirements. InCommon, a federation operator serving research and education communities, already had a mature set of identity federation systems and relationships that could be leveraged, as did Safe/BioPharma.

Use Case vs. Business Case

The construction of a trust framework and the government assessment criteria were highly iterative. Early on, FICAM met with potential vendors and representatives of the OIX, Kantara and InCommon to discuss its plans. Two issues emerged: privacy and the need for a business case for vendors. Policy-makers determined that IDM suppliers, who would normally be outside of the scope of the Privacy Act of 1974, should be enjoined to privacy requirements similar to the ones the agencies adhered to. Since the technical arrangement of federated identity would allow each IDP to know every place a citizen logged in, it was decided that IDPs were forbidden from disclosing anything they learned about a citizen's online activity, nor could they use the information for any purpose aside from federated identity (e.g., for marketing). Along with requirements for only disclosing the data an RP requests and the need for citizens to opt-in to the use of their data, FICAM released a set of requirements that trust frameworks were to enforce in service of citizen's privacy.

[10] Secure Assertion Markup Language, a framework for communicating authentication and attribute information. See http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security.

The second issue was more fundamental and has not yet been resolved. The FICAM view of the world was a set of *use cases* – it envisioned a number of situations where the American people interact with their government through the use of commercial identity providers. The benefits of the proposed system are to government agencies who, as described earlier, need strong authentication, and to citizens, who would gain value from broader, more varied, secure electronic interactions with government services. The use case view taken by the government is problematic though because it does not take into account the needs and logic of the market. Where FICAM saw use cases, would-be commercial suppliers sought *business cases*. That is, someone would have to pay for commercial actors to take part in the system. FICAM and others believed that there would be an inherent value to companies becoming IDPs; that there would be a commercial advantage in extending extant digital identities – such as Google and PayPal accounts – into the realm of E-Government authentication. Participating companies did not come to share this belief.

The first iteration of the FICAM trust framework arrangement sought to certify a group of IDPs at LoA 1 under the OIX banner. The vendors were allowed to self-certify. LoA 1 does not require verification of identity – all interactions are assumed to be pseudonymous – and security for the credential need not be greater than a password. This meant that the costs for a vendor to participate in LoA 1 certification were relatively low. Five companies were certified: Google, PayPal, Yahoo, VeriSign and Wave Systems[11]. However, since at LoA 1 there is little or no confidence in the identity asserted, it's unsuitable for transactions involving an exchange of personal data. For higher Levels of Assurance, there are significant costs involved in building systems that can verify identity and implement high degrees of security. For commercial companies to build such systems, market logic says there must be a return on investment – that there has to be a good business case. To date, no sustainable business case has emerged for companies to build systems for citizens to access government services. Only one company has certified above LoA 1, Verizon, a wireless and wireline communications company[12]. They have incurred the expense to

[11] See http://www.idmanagement.gov/pages.cfm/page/ICAM-TrustFramework-IDP.
[12] Another company, Experian, a credit reference, fraud deterrence and marketing information company, has a pending application at the time of this writing.

meet the requirements for Levels 2 and 3 because of business opportunities in the health sector. The LoA 2 and 3 credentials will not be used for citizen access to services – they will be used by doctors and other medical staff for electronic prescriptions and medical record access. The absence of a compelling business case for vendors to create credentialing systems above LoA 1 for citizens is a critical problem in the US plan to rely on external credentials.

Mixed Service Delivery

Trust frameworks are clearly a form of mixed service delivery, but of what service? There are two answers. First, though it is not a conventional public service, trust frameworks fill a gap in the *provisioning of identities.* In the US, many states offer ID cards so that residents may prove their identity or age in lieu of a driver's license. It can be argued that this is a public service for those who cannot or do not wish to possess a driver's license, the de facto form of ID in the US. In this light, the digital identities needed to access a variety of government and non-government services (as in the case of Verizon LoA-3 credentials for non-public medical record access) could be seen as a public service, though this point invites debate. The second answer is that, rather than providing a service *per se*, trust frameworks are a necessary precursor to accessing more traditional forms of public service. Authentication is a "lock and key" – the valuable part is what is on the other side of the door. If the authentication function of online public services is not worthy of being seen as a public service in its own right, then what's salient is the need to involve private actors to deliver services over the internet. In this we see echoes of the omnipresent public/private character of supplier relationships: government offices are rented from private landlords, public health programs buy drugs from private pharmaceutical companies, waste removal trucks may be serviced by private mechanics. Indeed, the most persuasive vision of trust frameworks is that they are part of a procurement process. What renders them a rich seam of research is that they effectively outsource a domain that has historically been the province of the state – citizen identification. This blurs the traditional line between official identity, such as a passport, and unofficial forms of identity, such as a debit card. If the state no longer holds a monopoly on the authenticity of our identities, then commercial logics must be considered in any analysis of their

changing nature[13]. To wit, FICAM's privacy requirements constrain a private company's impulses to glean all data from its customer-citizens in order to market more effectively to them. While some federated identity architectures are capable of "blinding" IDPs to the use of their credentials, this is not envisioned in the United States[14]. So, should the challenge of sustainable business cases be surmounted – and this is by no means definite – IDPs will know where all of their users log in. Contrast this with showing a driver's license or supplying personal information to an agency to authenticate; there is no private third-party "looking over your shoulder." Though federated identity addresses real problems, and in the US the trust framework model is being used to meet very difficult challenges in rolling out meaningful E-Government services, considerations of the changing nature of citizen-government relations and especially of privacy are both warranted and necessary.

Conclusion

This paper detailed the hybrid public/private nature of authenticating US citizens for access to online government services. In order to ensure the privacy of personal information, governments must know with whom they are interacting in an electronic environment. The paper discussed the federated identity model, where a single party acts as an Identity Provider for a citizen, and agencies become Relying Parties, consuming the credential issued by the IDP. The US must rely on organizations external to the government to act as IDPs because of a lack of an authoritative federal resource to authenticate citizens, and a strong, historic antipathy towards national identification. Though useful, the US government's vision of private companies acting as IDPs for citizens is challenged by those companies' basic need to get a return on their investments. It's unclear if the tension between use case and business case will be resolved in the near future.

References

ACLU (n.d.). Opposing Voices. *RealNightmare.org.* Retrieved April 26, 2012, from http://www.realnightmare.org/opposition/9/

Etzioni, A. Identification Cards in America. *Society 36*(5), 70-76.

[13] Cf. Lyon, D. and Bennett, C. (2008). Understanding the Significance of Identity Systems. In Bennett, C. and Lyon, D. (Eds.). *Playing the Identity Card*. Oxon: Routledge

[14] The issue of privacy-preserving architectures in federated identity management systems used for E-Government access is the general subject of the author's dissertation.

.gov Reform Task Force (2011). *State of the Federal Web*. Retrieved from http://www.usa.gov/webreform/state-of-the-web.pdf

OMB (2012). *Report to Congress on the Benefits of the President's E-Government Initiatives, Fiscal Year 2012.* Washington, DC: Government Printing Office.

Open Identity Exchange (2010). *What is a Trust Framework?* Retrieved 9 April, 2012, from http://openidentityexchange.org/what-is-a-trust-framework

United Nations (2005). *Civil Registration in Austria.* Retrived from http://unpan1.un.org/intradoc/groups/public/documents/other/unpan022349.pdf

West, D. (2007). *State and Federal E-Government in the United States, 2007*. Retrieved from http://www.insidepolitics.org/egovt07us.pdf