E-GOVERNMENT: PRIVACY MODEL

Dr. Hassan Aljifri, University of Miami, hassan@miami.edu
Dr. Alexander Pons, University of Miami, apons@miami.edu

ABSTRACT

E-government services are being adopted by many government agencies to better serve their citizens. The ultimate goal is to provide these services while taking into consideration the privacy of citizens' information and the security of its transmission. We propose a framework that aims at protecting the rights of individual citizens through the use of existing technology that facilitates the management and distribution of policies and procedures. Our single source and push methodology, coupled with Web Services, enables the deployment of an e-government system that will protect privacy, while at the same time be responsive to policy and procedure changes. The proposed Active Government System (AGS) combines the technologies of active database and Web Services to sustain the security of citizen information, while allowing for the convenient management and adaptability of the system to meet the ever-changing governmental environment.

Keywords: G2C, Active Government System, Privacy, Management of policies.

INTRODUCTION

The concept of "e-governance" refers to the transformation of traditional public sector services and processes into an electronic model with greater accessibility and interaction. E-government is the use of the Internet to bring together citizens, businesses and governments. The principles of democracy are further enhanced by the increase in government's availability to its citizens (2). The citizen becomes a more integral part of the democratic system when access to government is simpler and easier.

The complete design model for a government-to-citizen (G2C) centers on making it a one-stop integrated portal for government services designed to provide most of the services a citizen might need. Filing tax returns, voting, applying for a passport, and renewing a driver license are some of the services that should be provided by the G2C portal.

It is obvious that such a model would require the integration and the cooperation of different government agencies at the local, state and federal levels. The G2C framework not only focuses on providing and enhancing service delivery to citizens, but also addresses privacy and security issues; privacy of citizens' information and the security of information transmission. Security and privacy are widely acknowledged as one of the most essential elements of a successful e-government implementation (4). In this paper, we present a framework that protects the rights of individual citizens through the use of existing technologies.

THE ACTIVE GOVERNMENT SYSTEM (AGS) FRAMEWORK

The AGS system proposed in this paper forms the basis of a hierarchal structure of active databases (5) that propagate rules to protect the privacy of citizens, while allowing for an effective means of policy and procedure management. This system, coupled with adequate security measures, will facilitate G2C interactions that protect citizen's information according to policies and procedures established at the federal, state and local government levels. These policies and procedures are formulated into sets of database rules that protect the integrity of the information maintained in each respective database. The rules preside over what and how information can be exchanged among local agencies, local and state agencies, and local, state, and federal agencies.

G2C: An Example

Consider an individual applying for a position as a school bus driver. It is often required that a background check be conducted on this individual. With the AGS, once the individual is entered at the local level as a potential school bus candidate, local, state and federal rules are triggered to conduct a full and comprehensive analysis of the individual. Of course, the AGS should be aware of any privacy conflicts that protect individual rights, such as not conducting an IRS check in hiring an individual for a bus driver position. The advantage to the AGS is that it protects a citizen's privacy by blocking irrelevant information to other agencies or departments, while allowing full disclosure to the appropriate agency.

Proposed Model

The proposed model organizes the active databases (AD) into a hierarchical, tree-based structure (Figure 1). Each node in the tree corresponds to an AD; the AD could be a local, state or federal database. The node at the top of the tree is the root node. The ADs under that root are constrained by the rules and policies of that root; the subordinate ADs may amend rules with more restrictive policies, but not with more relaxed policies.
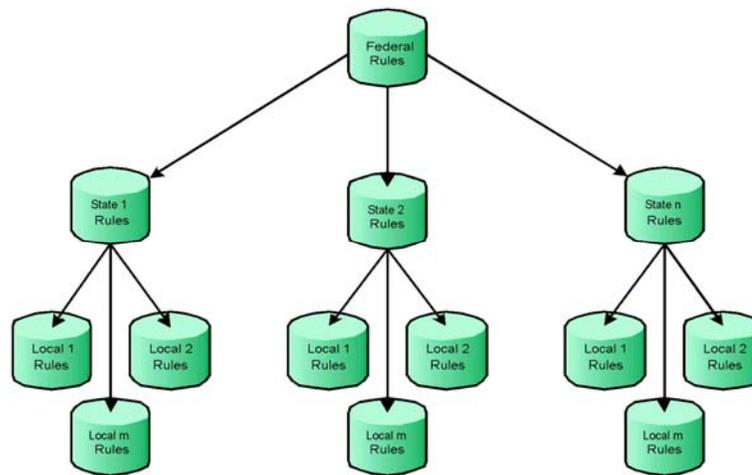

Figure 1. E-government rule management hierarchies

The root of the tree is the Federal Active Database Systems (FADS). It sets policies that all subordinate State Active Database Systems (SADS) must follow. The SADS, in turn, sets the policies for the Local Active Database Systems (LADS). These active databases serve as the repositories of citizen data, as well as the rules that must be enforced during data and information manipulation during portal access. The content and functionality of the various ADs are as follows:

- <u>FADS</u> – These databases maintain all federal information concerning the citizens of the country. Active database rules enforce polices and procedures according to the users' rights. At this level, database rules govern the exchange of citizen data among federal agencies. The rules are passed-down to all corresponding state systems.

- <u>SADS</u> – Information required for each citizen is maintained in these databases, including the rules which govern how a citizen's information can be manipulated among state agencies. At this level, database rules are passed-down to local systems within the state.

- <u>LADS</u> – All local citizen data are kept in these databases, which include rules that oversee the management of citizen data. The rules at this lower-level conduct citizen business at the municipal, county, or city level, but are restricted to operate within the SADS and FADS rules. In fact, any service engaged by the citizen will automatically trigger all relevant LADS, SADS and FADS rules to accomplish the requested task.

To understand how this works, suppose that the federal government changes a policy regarding the rules for acquiring educational scholarships. These rules would be updated at the FADS level and propagated to all SADS and in turn to all LADS. Such rules could specify how a state may distribute and the characteristic for qualifying for the scholarships; even indicating how state agencies may request or collaborate on utilizing a citizen's scholarship request. At the local-level, these federal rules could be augmented with current state rules that would restrict how local government agencies or even individual citizens may access these federal scholarships.

The use web of services and XML technology (1, 3, 6) allows the transportation of rules from local, state, and federal levels to individual portals in a manner that applies these rules uniformly. The management of rules is very important; rules are stored in a single location where changes will be pushed up to the federated active database systems (FADS). The use of push technologies alleviates systems lower in the AGS hierarchical from monitoring rule changes in a system higher in the hierarchy. When new rules are added or modified at a higher level in the AGS, these rules are sent to lower nodes by design to keep all systems current and up-to-date.

DESIGN SPECIFICATIONS

The AGS model is a three-layer hierarchy. The root is FADS, the second layer is SADS, and the third layer is the LADS. Conceptually, we think of each node in this hierarchy as a single entity; however, the backend of each node is a collection of nodes (active databases).
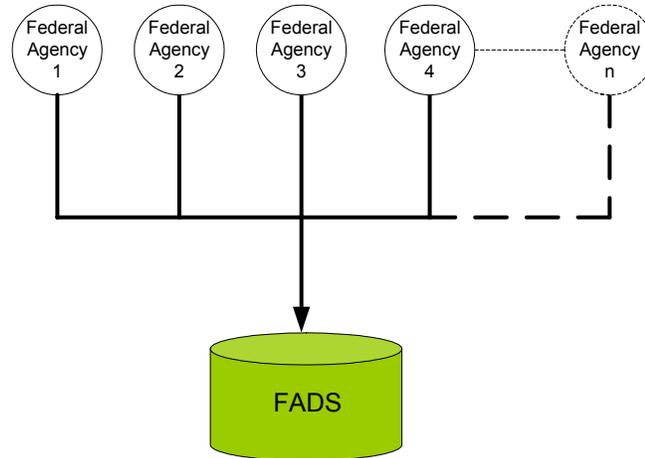
Figure 2. Management of rules in FADS

The FADS, SADS, and LADS are a physically linked, distributed group of database systems that comprise one logical entity. Although FADS is a single entity, it gets its unified data and rules from multiple sources. As Figure 2 shows, there is one location that handles the update and management of federal rules. The integration and the cooperation of all federal agencies are the building blocks of the FADS. The backend structures of SADS and LADS are similar to those of the FADS. All participating federal agencies publish descriptions of their services, network locations, and rules to the FADS using UDDI, which is used to describe the available Web Services in XML format. The state and local agencies publish their services using UDDI to the SADS and the LADS respectively. The rules in the higher layer are "pushed down" to the lower layers.

Application of Technology in E-government

The discussion below depicts how these technologies (Web Services and active database) interact to establish a unified presentation to citizens, while allowing for the effective management and maintenance of the e-government systems. Consider citizen Bob, which resides in state A from location A' within state A and is currently in location B' within state B. When Bob logs into the local portal in B', the e-government system automatically determines that he is from A' in A and gives him the government services of his area. Bob can conduct e-government tasks relative to this registered area or he may decide to access other local portals to conduct governmental tasks.

The system's intelligence establishes a single portal for the citizen to conduct e-government services in any area according to the rules of that area, but has the flexibility to allow him to perform governmental tasks in almost any area. Let's say Bob requires a hunting permit in his home state. Accessing these services from his current location, Bob would put in a request that would trigger checks automatically at the various governmental levels to determine Bob's status and his eligibility to obtain the permit. The system would check Bob's status at the federal, state, and local levels, while conducting and imposing any and all fees, regardless of Bob's physical location.

The goal of the AGS is to provide G2C services to citizens, while ensuring the security of the data and preserving their privacy. Figure 3 shows the publishing process and the requesting of services. The technology required for our system functions in the following manner.

- Local, State and Federal Authorities publish descriptions of their services and their rules using UDDI in LADS, SADS and FADS, respectively.
- Local, State and Federal Authorities describe the operations of their services using WSDL in LADS, SADS and FADS, respectively.
- Citizens access LADS using Message Exchange (SOAP) to locate the desired services.
- LADS check the availability of such a service using WSDL. The check is conducted locally, and at the state and federal levels.

To ensure the privacy of citizen information, the default setting is to hide the citizens' information from all government agencies at all levels. Thus, for an agency to be able to access a citizen data, it must specify the required data to be available and include such a request when it publishes its rules. Also, citizens can specify their privacy setting in their ticket. Such a ticket is used to accompany each request made by the citizens. The ticket contains the citizen's name and privacy credential.

Citizens must have full control over their privacy credentials. The ticket is matched against the rules specified in the node that provides the service. If a conflict arises, (for example, in order to furnish the citizen with the required service, it is required that the citizen must not block the service from viewing his/her SSN), a request is to be sent to the citizen for approval.
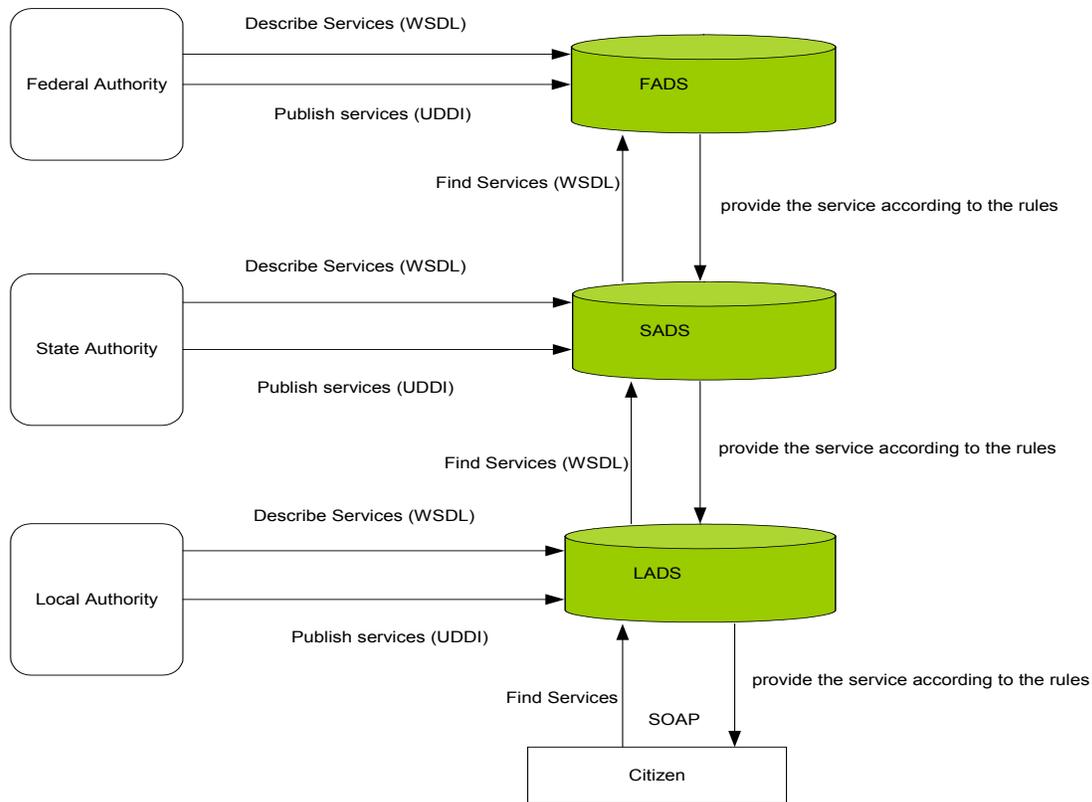

Figure 3. The publishing process and the requesting of services

11

ACTIVE RULES

Our system consists of rules that take the following form, which are required to perform checks concerning Bob's request for a hunting permit.

Rule 1: Citizen_Hunting_Permit_Register
Event:	Request state hunting permit
Condition:	Is citizen a state resident
Action:	Process request, check for state and local fees

Rule 2: Perform_HP_Training_Check
Event:	Citizen receiving hunting permit
Condition:	If citizen has not completed a hunting training course
Action:	Reject permit request and register citizen in a scheduled course

Rule 3: Federal_Felony_Check
Event:	State issuing hunting permit
Condition:	Check federal agencies for citizen restrictions
Action:	Identify and submit request to local state law enforcement agencies to conduct citizen interview

In the AGS there are many such rules to conduct government business. These rules are triggered and pass limited information in some cases to other rules for processing the citizen's service request. In our set of rules, if Bob has taken the hunting training course and has not been registered in the federal criminal system, he would be awarded a state-hunting permit once he has paid all applicable fees. Otherwise, rule 2 would request that Bob be registered for the course and would pass limited information to schedule him with the training agency, after which, Bob would obtain the desired permit. Rules 1 and 3 check for permit fees and outstanding federal warrants.

CONCLUSION

The development and expanded deployment of e-government encompasses many issues; but from a technological standpoint, we present a system, which when integrated with Web Services, is manageable and maintainable though policies and procedures may change at any level of government. The management of these rules utilizing the AGS will protect the privacy of citizens involved in the government process, while Web Services will establish the infrastructure of posting services, describing services, and securing the transmission of citizen information. The combination of Web Services and active database technology, as supported by the AGS, solves many of the problems that exist with e-government, primarily the protection of the citizens' privacy and the security of data transmission with e-government web sites.

REFERENCES

1. Atkinson, B., Della-Libera, G., Hada, S., Hondo, M. et al. (2002, April). *Web Services Security (WS-Security) Specification.* http://www.verisign.com/wss/wss.pdf

2. Backus, Michel.   (March 2001), *E-governance in Developing Countries,* IICD Research Brief – No 1

3. IBM Corporation (2002, April) *Security in a Web Services World: A Proposed Architecture and Roadmap*. http://www-106.ibm.com/developerworks/security/library/ws-secmap/

4. Medjahed, B., Rezgui, A., Bouguettaya, A. and Ouzzani, M. (2003). *Infrastructure for E-Government Web Services*, IEEE Internet Computing. pp. 58-65.

5. Widom, J. and Ceri, B. (1996). Introduction to Active Database Systems. San Francisco: Morgan Kaufmann Publishers, Inc.

6. Wong, W. (2002, June). *Sun switches gears on security.* http://news.com.com/2100-1001-939823.html