*W3C Workshop on e-Government and the Web,*
*National Academy of Sciences,*
*Washington DC, USA*
*18-19 June, 2007*

# Secure E-Government Portals

- Building a web of trust and convenience for global citizens

Anil Saldhana
Red Hat Inc
Anil.Saldhana@redhat.com

## Introduction

There are 4 types of e-Government services that are possible; Government to Citizens (G2C), Government to Businesses (G2B), Government to Employees (G2E) and Government to Government (G2G). In this position paper, I will focus on the Secure Portal possibilities for G2C.

Increasingly various governmental agencies are providing services to its citizens via dedicated web sites. As a citizen requiring services from the local, state or federal government, I rely on these separate web sites not only for information but also to avail services like filing tax returns, renewal of license plates/vehicle stickers, communicate with the county for property tax issues etc. Providing a single secure portal that acts as a window to the various services is beneficial not only to the government but also to its citizens. In this position paper, I describe the need for a secure portal, current sample usage of online services by US governmental agencies, an example of an ideal web experience for a citizen to use E-Government services, the challenges and possible solutions to creating secure E-Government Portals for global citizens.

## Benefits of a Secure Portal

The benefits of a Portal are immense. Portals act as a one stop resource for information. Having a secure e-Government Portal will reduce the costs for the government in delivering timely information to its citizens. The citizens will also benefit from timely and readily available information as well as a medium to avail services. Having a web portal will reduce the need for dedicated governmental representatives to be available by other modes of communication like Phone or email to provide information to citizens. It will be much simpler and cost effective for Governmental Representatives as well as the Representatives in governmental legislation bodies like the Senate and the Congress to get in touch with the citizens to pass information on important legislations, Citizen action items etc.

## Examples of usage of online services by US Governmental Agencies

The US Social Security Administration [1] projections for online visitors for FY 2006 were 52 million out of which 29 million would view the Frequently Asked Questions

(FAQ) section and 650K email inquiries would be expected. If you cherish the notion that only the young are web savvy, then [1] puts the misconception to rest stating that senior citizens are the fastest growing online audience, who will double by 2010. This report also declares the intent of the SSA to reduce the number of paper W-2 statements received from 4 million employers by fostering online submissions.

According to Nielsen Internet Research [2], the number of visitors to the United States Internal Revenue Service (IRS.gov) website was 13,590,000 unique in the month of March in 2007. Just imagine catering to these visitors by any means other than the web.

## Example Use Case

The following is a Use Case that describes an ideal usage of an E-Government Portal with a trust context in-built in the portal:
The day is April 8, 2007, a Sunday. At 9am, Anil logs into the e-Government portal for the state of Illinois. He scans through the general informational alerts and other information on the main page. He goes to the section on the main page that asks him to login. He enters his username and password. He is provided a personalized page that contains a section for personalized alerts via RSS feeds. Today, the RSS feeds include alerts that inform him that the deadline for tax returns filing is April 17$^{th}$. He also sees an invitation from his local congressman to attend a local town hall meeting on April 25th. He decides to check for potential replies to the email he sent to the Cook County Tax Assessors office regarding some issues with his property records. He clicks on the section for Cook County.

He is taken into the Cook County portal where he clicks the email link. He is asked a couple of security questions that were preconfigured during registration. Once he has answered them, he is taken to the email agent on the web where he opens the email from the tax assessor's office. He obtains the necessary information from the email. He logs out of the email client. He is taken back to the cook county portal. He clicks to go back to Illinois state portal. He is satisfied with the e-Government portal for allowing him to perform some business with the government, on a Sunday.

It is April 13$^{th}$ and it is 10pm, Anil has decided to submit his tax returns both to the federal agency as well as the state agency. Again the Illinois State portal will act as the front door to both. He logs into the Illinois state portal with plain user name and password. There is a link for the federal tax filing. He clicks on it. He is redirected to the secure IRS website where he is asked additional questions as well as provide an opportunity to enter his social security number, the previous years gross income and a mutually agreed upon key. He is presented with an online tax software process which will walk him through the filing process. Once he has filed his federal return, he is presented with links to the state agencies where he will need to file his state tax returns. Anil files his state tax returns. The whole process has taken him under 30 minutes. He logs out and goes to bed satisfied.

## Collaborators for a Secure e-Government Portal

The parties involved in the successful deployment and operation of a secure e-Government Portal are the citizens or end users, browsers as the technological clients, the Governmental agencies as the source/sink of information and the technology companies/standards that provide secure communication between the client and the server.

Since the involvement of humans in a secure environment is error-prone, there is a need to delegate as much security responsibility as possible to technology. I propose that there be a technical trust established between the client agent (browser) and the server agent (Government server). This trust can be established by technology embedded in the browsers that recognize trusted web sites.

If a particular URI emanates from a trusted government web site and leads to an un-trusted web site, then the browser should not allow the request to pass through. All the communication that happens between the browser and the server has to be shielded from man-in-the-middle attacks. Hence PKI/SSL is a must for all government web sites. If the cost of public-key cryptography is a limitation and the services provided do not need the utmost level of security, then alternative technologies or standards that provide comparable transport level security, like the Secure Remote Password (SRP) [5] should be embedded in the browser and all server software hosting the government websites. If XML based technologies are adopted, then technologies like web service security with XML encryption and XML signatures can be used between the browsers and the service providers.

In summary, the user should not be worried about any security in using the E-Government Portals. The browser technology, the transport technology and the E-Government Server designers have to make sure that the end user is relieved of any security concerns.

## Challenges

The challenges facing secure e-Government Portals are many.

One of the primary challenges is to get a buy-in into a single IT installation from the various departments and organizations of a Government. The following statement by the Australian Prime Minister sums it up [3]:

*"Another challenge is the capacity of departments to successfully interact with each other in pursuit of whole of government goals and more broadly, for the entire Service to work in partnership with other bureaucracies, with business and with community groups as resources and responsibility are devolved closer to where problems or opportunities exist."*

- Hon. Jon Howard, Prime Minister, Centenary of the APS Oration, 2001

The practical architecture for E-Government portals seems to be one involving a **Service Oriented Architecture** (SOA), where in the portals make use of web services provided by other governmental agencies/partners over secure channels.

The other challenge is the management of security related data for the citizens. A federated identity model can be adopted by the e-Government portals that work as follows: there are one or more authentication providers that work in the background for these secure portals. When the citizen accesses information that needs additional level of security, then the e-Government Portal can redirect the citizen to the authentication provider and on successful authentication, is redirected back to the e-Government website. OpenID [6] is a good candidate.

If E-Government portals have to create a trust context among the citizens to enable them to use the web for sensitive transactions, then the portals have to provide the confidence to the citizens that they do not have to worry about any security when doing the sensitive transactions. Getting the citizens to use the web for Governmental services is not a big issue because the online usage is increasing. It is only when the browser technology advances to incorporate trust notions, is when people are going to feel safe about using the browsers for sensitive transactions.

## Possible Solutions

- *Increase Online Usage:* Provide incentives to citizens to use the web for paid governmental services (reduced Vehicle Stickers/License Plates renewal, discount of $100 on Property Taxes). An Offer for free online tax returns has hugely increased online activity for the IRS in 2005 as evidenced by this report [4], which also states that out of 120 million expected tax filings online, 88 million had been turned in by April 8 2005, a week before the deadline.
- *In-built security context in the Portals:* Define varying levels of security for the E-Government services provided online. General public information has zero security, personalized content with read-only links with user-id and password usage and usage of multi factor authentication for sensitive operations like tax returns filing, social security information etc. When the citizen uses user id and password, he or she is presented with a portal page that contains personalized content for the local, city or state level with messages from the county, state or federal legislators, mayors etc. If the user has a need to access sensitive information like SSN, Military Service records etc, he is solicited multiple information along with the initial user id and password. The more sensitive the information, more the number of hops the user needs to cover. The additional levels of security that is in built into the portal will give the web user confidence in using online services to make sensitive transactions.
- *Marketing Secure E-Government Portals:* Free seminars should be provided to citizens to get acquainted with the secure features of the online e-Government portals.

## Conclusion

The number of users of the internet is growing rapidly around the world amidst growing concerns of security and privacy. With the advent and progress of internet security standards and technologies, the concerns are being handled. It is natural for Governmental agencies to embrace the online infrastructure to deliver content as well as services to their citizens. With the proper choice of secure technologies and adequate training and awareness, it is possible to have secure E-Government portals operating at various levels of the government.

## Reference

[1] *'Effective eServices at SSA'*, Office of Electronic Services, Social Security Administration, (http://www.usa.gov/webcontent/documents/effective_eServices-09-19-2006.ppt )
[2] Nielsen/ NetRatings (http://www.netratings.com/press.jsp?section=newsletter)
[3] Australian Government use of information and communication technology (http://www.apsc.gov.au/mac/technology.htm)
[4] *'Tax-Related Web Sites captured 7.6 Million Internet Users This Past Week'*, (http://www.internetadsales.com/modules/news/article.php?storyid=5283)
[5] SRP-Open Source Password Security (http://srp.stanford.edu/ )
[6] Open-Id: Decentralized Distributed User-Centric Identity (http://openid.net/ )

## About the Author

Anil Saldhana is the Project Lead for JBoss Security and Identity Management, JBoss Division, Red Hat Inc. He represents JBoss/Red Hat at the JCP, W3C and Oasis standards organizations. He is also an active member of the Apache Program Management Committee for Web Services at the Apache Software Foundation. He speaks frequently at conferences on topics related to security and software.