International Conference on eBusiness, eCommerce, eManagement, eLearning and eGovernance 2015 [IC5E 2015]

ISBN	978-81-929742-8-6	**VOL**	1
Website	www.ic5e.org	**eMail**	ic5e2015@ic5e.org
Received	01 - January - 2015	**Accepted**	30 - May - 2015
Article ID	IC5E012	**eAID**	IC5E.2015.012

A Centralized Multimodal Authentication Platform with trust model approach for securing federal e-government budgets services and applications

Sea Chong Seak[1], Zulkfli Bin Ahmad[2], Wong Hon Loon [1]
[1]Information Security Lab, MIMOS Berhad, Kuala Lumpur, Malaysia
[2]Information Technology division, Ministry of Finance, Putrajaya, Malaysia

Abstract: *In recent years, there has been rapid growth of e-government services & application go on web. Malaysia federal government enable national budget services and application online for more efficient on managing, planning, monitoring, evaluation and accountability. The information and data was used by the application are high confidential and very important for country. The need to develop strong policy and technical mechanisms to improve the security of and enable secure communications for applications on the web. One of the research output from local research institute (MIMOS) was identify and deployed to enhance and protect the system and confidential data. Centralized multimodal authentication platform with trust model approach was used to secure and protect the federal e-government budgets services and applications.*

I. INTRODUCTION

Recently, most of the government around the world including Malaysia government have initiated their e-government strategies to exploit and use Information Communication Technologies (ICT), e-commerce models and best practice to fully integrate most of the e-government services and turn in online. The main objective is to improve the government operations and support citizens through use of web technologies to public sector and e-government digital contents.

One of the Malaysia government effort and initiative is use ICT & best practice to increase efficiency and effectiveness of the national budgets system and programs. The outcome based budget (OBB) system was developed with a well-structured national level strategic plan lays the foundation for focused sector and program levels plans and allow ministries and departments to establish linkages to higher-level key results areas. Part of the functional on this system provides baseline data that allow measurement of comparable progress and results at predetermined intervals. Performance data are explicitly focused on measuring performance progress areas such as key result areas (KRAs), goals, objectives, outcomes, outputs, and activities. Such performance data are monitored against predetermined targets. This budgeting system is critical to meeting Malaysia's national needs and the challenges of globalization and regional competition.

When the e-government critical and important system such as outcome based budget system go online and accessible via public network, the increases and need of regulatory security requirements for the protection of confidential data and strong authentication to measure the authorization personal only can accessible to the resources and confidential data. The e-government services providing their citizen services and offering internet-based services should use secure and efficient methods of authentication to protect the confidential data.

Cite this article as: Sea Chong Seak, Zulkfli Bin Ahmad, Wong Hon Loon. "A Centralized Multimodal Authentication Platform with trust model approach for securing federal e-government budgets services and applications." *International Conference on eBusiness, eCommerce, eManagement, eLearning and eGovernance* (2015): 104-108. Print.

Accessing today's most of the e-government web-based online system requires a user friendly and convenience methods which is depend on username name & password to authenticate the user identity. This methods is a significant vulnerability since the user password can be easy captured by the man in the middle attack and later used for making illegal access to the user account.

II. BACKGROUND

The Outcome based budget (OBB) system was introduced and has been established in the Ministry of Finance Malaysia in year 2011 [1]. Malaysia is not a first country in reforming the budgeting system, OBB has been successfully implemented in a number of countries such as Canada, Singapore and New Zealand. Malaysia introduce and implemented of OBB can be seen as another effort by the Malaysia government to reform the budgeting system to better manage and achieve results. It success will hinge upon translating the theory into practice with cooperation of all in the Malaysian public sector. OBB also will ensure value for money when duplication of resources across ministries is eliminated. The estimated benefits obtains from OBB included online budget preparation, analytical reporting on budget usage and results, integration of workflow management and audit trails.

Under OBB, the application named "MyResults" [2] URL (https://www.myresults.gov.my/) was developed not solely for the preparation of the budget, but as a strategic planning tool and public sector performance management comprehensive. MyResults provides users with framework structures for monitoring& evaluation, online budget submission, review & verification, performance monitoring and reporting. With MyResults application, all the ministry will have an online access to information about its program objectives, resources utilization, activity completion, output generation, outcomes and impact achievement from the system and also can be used for evaluation purpose.

Authentication is a complex problems. E-government systems need to authenticate users to back-end data sources and applications, yet these applications may each have different underlying security infrastructures. And the ideal and most efficient authentication solution is a single sign-on one, or SSO, in which the user only has to log in once and is authenticated to all of the network resources. Many techniques for authentication don't work or don't work very well for Internet based applications. In this discussion, my goal will be to describe some of the high-level challenges and solutions found in implementing a national centralized multifactor authentication and Single-Sign-On for e-government web based applications. The desired scenario for e-government authentication framework with multiple web applications require optimized and centralized multi-factor authentication with single sign-on capabilities across a wide variety of e-government services and functions.

V. UAP SYSTEM ARCHITECTURE

The centralized multimodal authentication system based on new authentication platform that is provide both secure and highly usable. With combination of our trust model approach to enforce another security level even though use with the traditional username password authentication method. The system provides a highly secure environment that is simple to use and deploy with the limited resources that does not require any change in infrastructure and communication protocol.

To adopt UAP trust model approach & adaptive authentication features, application developers need to modify and separate the authentication module and rely on the central module as the main source. This is what we mention early advised de-couples authentication mechanism from application. This is moving towards a trusted model where a central application handles all types of authentication for an organization.

I. Trust Model Approach

Using UAP, application can define required trust level while UAP system evaluates user trust level based on authentication methods used. User is only allowed to login to application if the evaluated trust level exceeds application required trust level.

II. Adaptive Authentication

User is required to provide additional authentication if the trust level is less than application required trust level.

V. DEPLOYMENT MYRESULTS APPLICATION AND UAP SYSTEM

UAP and MyResults application already deployed as production few years ago but recently deployed with our trust model approach. In this section, we have defined and explains two different type of MyReults application system architecture. One model configure as low trust model which sufficient for basic security requirements and other model configure as high trust model to be establish as high security requirement.

With trust model approach, MyResults application can define required truest level and while UAP authentication server evaluates user trust level based on authentication methods used. Users is only allowed to login to MyResults application if the evaluated trust level exceeds MyResults application required trust level.

According to our best practice on assigning the weightages on trust level, the authentication methods or credentials are ranked based on their security strength and given weightages system also allow application to have different requirement trust level. In current production server, UAP system have turn on three authentication methods, which are password, OTP token and SMS OTP.

a. Password.

The most basic authentication method relied on the user chooses it and something that fits in the memory of a user. This method of authentication is about verifying the user physical identity remotely, and the user behavior is necessarily involved throughout the process. Trust level assign to this authentication method is with value 13.

Cite this article as: Sea Chong Seak, Zulkfli Bin Ahmad, Wong Hon Loon. "A Centralized Multimodal Authentication Platform with trust model approach for securing federal e-government budgets services and applications." *International Conference on eBusiness, eCommerce, eManagement, eLearning and eGovernance* (2015): 104-108. Print.

b. OTP Token

A password that is valid for only one login session or per single transaction. OTP numbers are difficult for human beings to memorize. Therefore, they require additional technology and hardware token in order to work. OTP device creates a "two-factor" security system which means you'll have to know something (your user name) and to have something (the OTP security token) in order to login into the authentication. Trust level assign to this authentication method is with value 20.

c. SMS OTP

The method used to authenticate user based on the non-reusable random generated mobile Short Message System (SMS) OTP deliver to a user via SMS. Mobile SMS OTP will only be valid per login session. This method also creates a "two-factor" security system, which the mobile SMS OTP and the user mobile phone to receive the mobile OTP via the SMS network. Trust level assign to this authentication method is with value 18.

A. UAP and low trust MyResults Application System Architecture

UAP with the trust modal approach provided better security protection for users and application. We have successfully deployed this new architecture for MyResults application with UAP. Figure 5 shows the detail flows of UAP low trust model with MyResults application system architecture and also how UAP provided security protection to the applications. In the system architecture diagram Figure 1 show the trust level of MyResults Application set it to value 10, for the three authentication methods trust level value already define above this section.

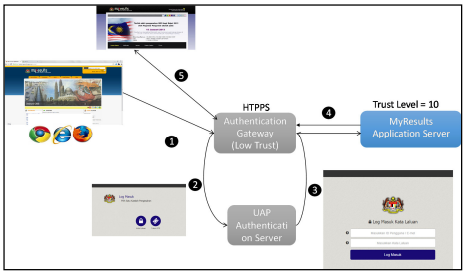

Figure 1: UAP Low Trust model with MyResults Application System Architecture

Let's begin with the user access to MyResults application via the URL https://www.myresults.gov.my. The user arriving at the UAP gateway which configure as Low Trust model. We assume the user reached the gateway without an existing session and without any information about the user identity. Information about user identity is sent from UAP authentication server to UAP gateway which prepared the information for protection information contents use by applications.

For better understanding, the author describe the system architecture with step by step transaction flows from beginning until authorized user granted access protected resources. For this trust model approach, we use the trust level defined early which included trust level for authentication methods and MyResults application.

1. User accessing the MyResults application and user arriving at UAP gateway. UAP gateway unable to detect the authentication session, UAP gateway will redirect to UAP authentication server via user browser.
2. When user redirect to authentication server, the authentication server present the authentication page for user to choose prefer authentication methods login to the system. In this deployment, low trust gateway configured and make available only password and OTP token authentication method.
3. If the scenario user choose the password authentication method and successfully provided the credential for authentication, user will redirect back to UAP gateway via browser.
4. When arriving UAP gateway, UAP gateway will do verification and evaluation on trust level requirement between users choose authentication method and MyResults Application. In this case, trust specification require for MyResults application is set to minimum trust level 10. Trust established based on authentication input, this scenario user authentication input is password which carry trust level 13.
5. In this scenario, the user authentication evaluation result exceeds the minimum security requirement of MyResult application. This mean that user can access MyResults application & resources with the user's permission granted by application and based on trust level up to the application trust specification.

B. UAP and high trust MyResults Application System Architecture

We assume the user reached the gateway with an existing session and information about the user identity. Information about user identity is sent from UAP authentication server to UAP gateway which prepared the information for protection sensitive information contents use by applications. Figure 2 shows the UAP high trust model with MyResults application system architecture which deployed for security protection on sensitive data and application resources. In this scenario high trust model, the security requirement for MyResults application trust specification set it to trust level 30 which is higher compare with low trust model.

Cite this article as: Sea Chong Seak, Zulkfli Bin Ahmad, Wong Hon Loon. "A Centralized Multimodal Authentication Platform with trust model approach for securing federal e-government budgets services and applications." *International Conference on eBusiness, eCommerce, eManagement, eLearning and eGovernance* (2015): 104-108. Print.

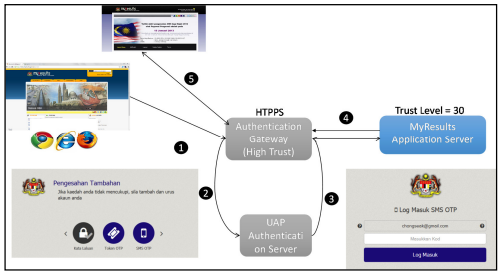

Figure 2: UAP High Trust model with MyResults Application System Architecture

In this scenario, we use the same trust level defined early for authentication methods and also MyResult application high trust security requirement trust specification defined in Figure 2. We create a scenario, user already authentication and granted access MyResults low trust application. When the user require accessing the sensitive resources or doing approval activities, MyResults application will redirect user to accessing the high trust UAP gateway. Below is the detail steps how the users being redirect to UAP high trust gateway and evaluation the security requirement and grant access to sensitive resources.

1. User accessing the MyResults application and user arriving at UAP high trust gateway. UAP gateway able to detect current authentication session and user identity, user is required to provide additional authentication because current authentication method trust level is less than application required trust level. UAP high trust gateway will redirect to UAP authentication server via user browser for additional authentication.
2. In this scenario, user already authentication using password but current input authentication method cannot meet the MyResults high trust application minimum security requirement specification. For this deployment, extra authentication method which is SMS OTP make available for user to choose when UAP authentication system require user for second authentication. The previous authentication methods already used will mark and cannot be used as second authentication. In the case, user choose SMS OTP method for second authentication.
3. User prompt for enter SMS OTP value which send by authentication server to user mobile phone via SMS. If user successfully authenticated, user will redirect back to UAP high trust gateway via browser.
4. When arriving UAP high trust gateway, the gateway will perform verification and evaluation on trust level requirement between users choose authentication method and MyResults application. In this case, trust specification require for MyResults application is set to minimum trust level 30. Trust established based on the first authentication input password carry trust level 13 and second authentication input SMS OTP carry trust level 18. In this scenario, total trust value for user authentication after successfully additional authentication is increase to trust level 31.

   5. In this scenario, the user authentication evaluation result exceeds the minimum security requirement of MyResult application. This mean that user can access MyResults application and access to sensitive resources or approval pages with the user's permission granted by application based on trust level up to the application specification.

VI. CONCLUSION

To adopt UAP, application developers need to modify and separate the authentication module and rely on the central module as the main source. This is moving towards a trusted model where a central application handles all types of authentication for an organization. User is required to provide additional authentication input if the trust level is less than application required trust level. User is only allowed to login to application if the evaluated trust level exceeds application required trust level.

With this model, new authentication method can be added without any modification to all the applications. Existing authentication method with newly discovered vulnerability can be disabled instantaneously, time responsive to threat will decrease. Successfully deployed UAP with MyResults application, Ministry of Finance Malaysia confident with enabling other MOF related e-government applications using UAP authentication platform with trust model.

ACKNOWLEDGMENT

We acknowledge the support provided by Ministry of Science, Technology and Innovation (MOSTI) in funding MIMOS Unified Authentication Platform (UAP) project through the Tenth Malaysia Plan (10MP). The completion of the project allows the delivery of a centralized authentication infrastructural platform for web applications.

REFERENCES

1. Mohd Sakeri Abdul Kadir, "Moving Towards Outcome Based Budgeting an integrated approach to planning, budgeting, monitoring & evaluation," Gov CFO summit 2002, 12-13 July 2012, Chiang Mai, Thailand.
2. Richard Barahim, "Integrated e-System for Whole-of-Government Performance & Budget Management" MES Evaluation Conference 2012, 10- 11 Sept 2012, Kuala Lumpur, Malaysia.
3. OASIS, "OASIS Security ervices(SAML)TC", https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
4. Gross, T, "Security analysis of the SAML single sign-on browser/artifact profile", pp. 298 – 307, Computer Security Applications Conference, 2003. , pp. 298–307
5. Sea Chong Seak, Ng Kang Siong, Wong Hon Loon, Galoh Rashidah Haron, "A Centralized Multimodal Unified Authentication Platform for Web-based Application," *WCECS 2014 The International Association of Engineers, October 2014, San Frabcisci, USA.*.

Cite this article as: Sea Chong Seak, Zulkfli Bin Ahmad, Wong Hon Loon. "A Centralized Multimodal Authentication Platform with trust model approach for securing federal e-government budgets services and applications." *International Conference on eBusiness, eCommerce, eManagement, eLearning and eGovernance* (2015): 104-108. Print.

6. Jrstad, I. ; Jonvik, T. ; Do Van Thuan, "Strong authentication with mobile phone as security token," *IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, 2009, Macau*.
7. Matbouli, H. , Gao, Q. , "Strong authentication with mobile phone as security token," *International Conference on Information Technology and e-Services (ICITeS), 2012.*
8. Nawaf Alharbi, Maria Papadaki and Paul Dowland. , "Security Challenges of E-Government Adoption Based On End Users' Perspective," *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014).*
9. Bakar, K.A.A. , Haron, G.R., "Adaptive Authentication: Issues and Challenges," *World Congress on Computer and Information Technology (WCCIT), 2013.*

Cite this article as: Sea Chong Seak, Zulkfli Bin Ahmad, Wong Hon Loon. "A Centralized Multimodal Authentication Platform with trust model approach for securing federal e-government budgets services and applications." *International Conference on eBusiness, eCommerce, eManagement, eLearning and eGovernance* (2015): 104-108. Print.