ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

Resolution Database Privacy preserving based Single-Sign-on Solution

S.S Dhanvantri Divi[1], T.Swapna[2], K.J.Sharma[3]

[1] Student, TRR ENGINEERING COLLEGE, PATANCHERU, HYDERABAD

[2] Associate Professor, TRR ENGINEERING COLLEGE, PATANCHERU, HYDERABAD

[3] Professor & Head of Dept, CSE, TRR ENGINEERING COLLEGE, PATANCHERU, HYDERABAD

Abstract: Now a day's information extraction from web is the main aspect in accessing services. User interested in single login with different resources and accessing provided services. Due to this requirement traditionally we are using Single-Sign-On solution for using different resources. Single-Sign-On solution is a popular technology allowing users to identify and authenticate once and gain access to different resources in a distributed computing environment. This has basically been achieved by implementing a secure exchange of ssPINs between trusted identity providers. The applied modifications and improvements do not harm the security and privacy preservation capabilities of the Austrian eID based authentication framework. At the same time, the developed solution satisfies also the predefined requirements for scalability, transparency, and user centricity. There is no restriction in providing services efficiently in single-sign-on solution. We have a plan to extend the above process can be worked in piloting phase. No server issues were faced in this phase. To increasing the security considerations in resources is the main advantage of our requirement. We are developing above requirement in resolution management system. The incorporation of gained experiences of this piloting phase and the integration of our solution in further productive applications.

Index Terms: Resolution Database System, Authentication Engine, SSO; identity management, privacy, Austrian citizen card, MOA-ID.

I. INTRODUCTION

Present days more number of users are gained protection information and resources from online with different authentication resources services. Single sign-on (SSO) is a property of access control of multiple related, but independent software systems. With this property a user logs in once and gains access to all systems without being prompted to log in again at each of them. Conversely, Single sign-off is the property whereby a single action of signing out terminates access to multiple software systems. As different applications and resources support different authentication mechanisms, single-sign-on has to internally translate to and store different credentials compared to what is used for initial authentication. we present a security architecture that fills this gap by enabling SSO between different administrative sectors using MOA-ID still as identity provider (IdP). We achieve this by enhancing MOA-ID and by transforming sectoral identifiers using an additional

ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

attribute provider (Source PIN Register Authority) hosted by the Austrian Data Protection Commission.

Secure and efficient decision making processes are of particular importance especially for small and medium-sized enterprises. In this context, delocalization of responsible decision makers often leads to decision making processes relying on circular resolutions. Although circular resolutions based on written consent are usually efficiently manageable for a limited number of decision makers, involving a potential large number of persons inevitably complicates these processes in practice. In this paper, a circular resolution database system that addresses this problem is introduced.

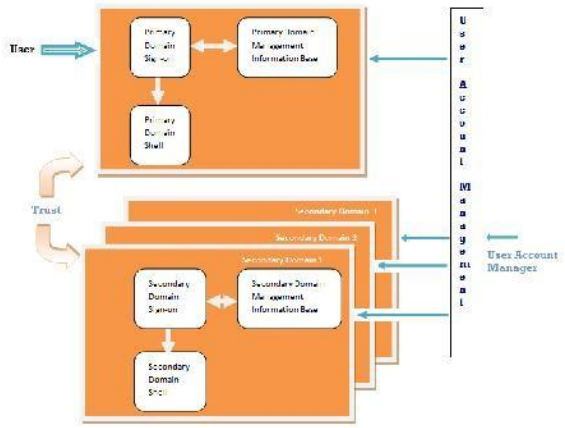

Figure 1: Single Sign-on services based data delivery.

Our solution, which is based on the Austrian citizen card concept, makes use of qualified electronic signatures that provide means for secure authentication of users as well as for electronic signing of digital documents. By enhancing decision making processes in terms of security, usability, and effectiveness while assuring auditing acceptability, the presented circular resolution database system especially contributes to the future competitiveness of small and medium-sized enterprises.

II. BACKGROUND WORK

Single sign-on exists and beneficial for all web users, because it encourages them to use a single authentication credentials in multiple domains. Reduces the burden of maintaining multiple authentication credentials. Sectoral (different domains) Identity Management (MOA-ID) has not been Single Sign-On-capable. Single Sign-On usage between different governmental applications where security and privacy for information accessed has utmost importance, existing systems fails to keep up these parameters (security and privacy) due to their inability to support Single Sign-On. So a better system is required that offers all the benefits of Single Sign-On based authentication yet preserving security and privacy aspects across different domains. Uses Single Sign-On (SSO) based architecture across different domains preserving security and privacy. Terms a Single Sign-On ID as MOA-ID for the current application context. Sectoral Identity Management (MOA-ID) is extended to be transformed to Single Sign-On-capable.

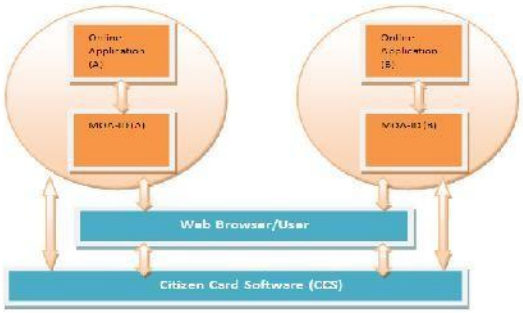

Figure 2: Current Cross-Sector Authentication.

Presents a security architecture that enables Single Sign-On between different governmental applications using MOA-ID as identity provider while meeting the requirements for sectoral data privacy protection at the same time. Achieves this by

ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

transforming unique sectoral identifiers of users with the help of an additional trusted attribute provider implemented using SSO protocol.

III. PROPOSED APPROACH

Provision of written consent can be cumbersome Satisfying security requirements can be difficult. So the better system is required for doing piloting phase in various resolution database management applications.

Austrian Citizen-Card Concept

Citizen-card is used in Austria to authenticate citizens over the Internet, e.g. in e-government processes. Citizen-card concept is based on qualified electronic signatures. Citizen-card concept is used to improve the processing of circular resolutions Electronic signing of resolutions Secure user authentication.

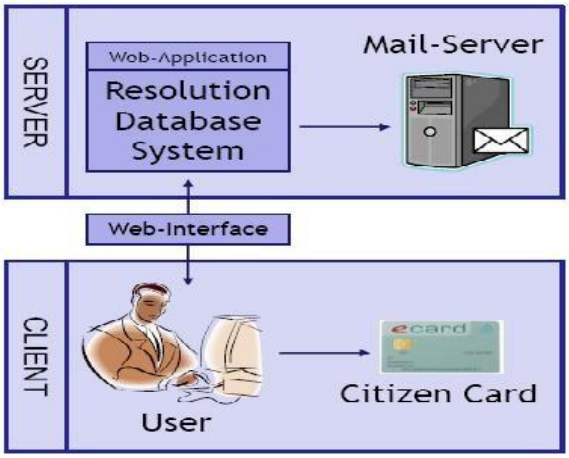

Figure 3: System Overview.

System Architecture can be achieved in resolution of piloting phase notification in providing services.

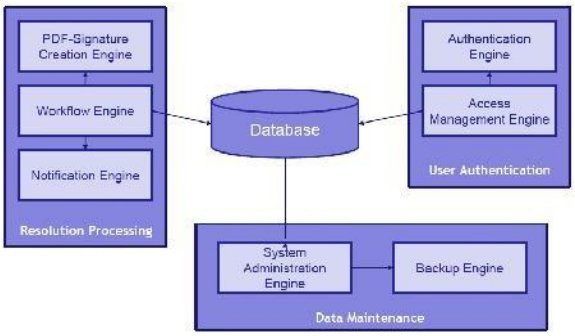

Figure 4: Resolution database management system.

Data Maintenance:

System Administration Engine User profile administration User privilege administration Document administration

User Authentication:

Access Management Engine Controls access to resources and functionality. Authentication Engine Authenticates users using the Citizen Card Based on functionality provided byan open-source framework.

IV. SSO Protocol

The process has four main steps for doing individual assurance of the security in the network. We assume that the user already been successfully authenticated once using her/her citizen card at MOA-ID (A). For that, we enhanced MOA-ID in such a way that a user's authentication session isn't immediately discarded upon ticket devaluation by the online application.

ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

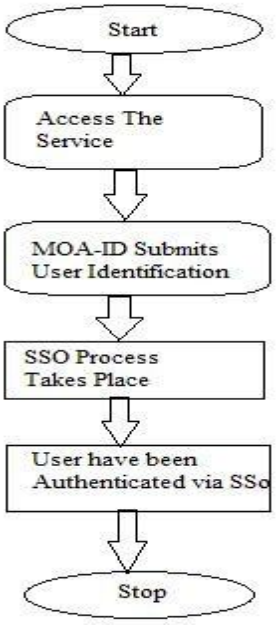

Figure 5: SSO Architectural Process.

Step 1: In this step, the user wants to access a particular service of sector *(B)* although currently interacting with an application of sector *(A)*. Instead of being directly forwarded to application *(B)* the user is redirected to MOA-ID *(A)* in order to check if she has been already successfully authenticated before, i.e. if the authentication session is still valid.

Step 2: If the requirements of Step 1 are fulfilled, MOA-ID *(A)* submits the user's identification data (name, date of birth), ssPIN (A) and SCB to the SRA for the calculation of ssPINenc (B).

Step 3: In this step the actual SSO process takes place. Since the user has been successfully authenticated before, the information of this previous authentication including ssPINenc (B) is packed into a SAML assertion and digitally signed. This assertion is based on SAML 2.0 and assembled according to the Web SSO profile.

Step 4: After having verified the assertion, MOA-ID (B) decrypts ssPINenc(B) with its private key RSApriv(B) and prepares the identification data to be sent to the protected application (B). The communication between MOA-ID (B) and application (B) is based on the SAML Browser/Artifact Binding 1.0. Although the SAML assertion transmitted between MOA-ID (A) and MOA-ID (B) is based on SAML version 2.0, the identification data sent from MOA-ID (B) to application (B) is still included in SAML 1.0 assertions.

V. RESOLUTION DATABASE

In this section we are using Berkeley Database for resolution database management. Transactional storage system for key/data pairs. "Embedded" indicates that Berkeley DB is a library linking directly into an application's address space, avoiding the costly IPC that reduces performance for client/server systems. On a commodity x 86 platforms, Berkeley DB returns millions of key/data pairs per second. Berkeley DB is scalable in a number of dimensions: it is used to store bytes to terabytes; its replication is used in systems. ranging from two to many tens of sites; it can be used as a simple data repository or as a highly concurrent, transactional engine. Berkeley DB provides both keyed and sequential lookup. It does not support any data model (e.g., relational or object-oriented), but

different data models can be implemented on top of it. Its simple storage model provides applications with the flexibility to store data in whatever format is most convenient.

IV.PERFORMANCE ANALYSIS.

In this section user register in to main server then he/she access services from that server.

ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

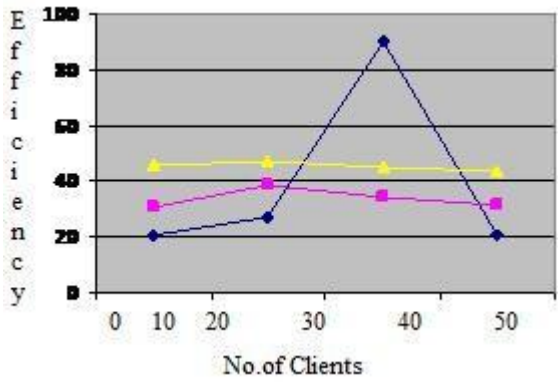

Figure 6: Performance results of server services in different systems.

As shown in above figure we are giving inputs as a login details for accessing details. Single user can access different system services with same user details using our proposed work in the resource database management systems.

VI. CONCLUSION

Uses Single Sign-On (SSO) based architecture across different domains preserving security and privacy. Terms a Single Sign-On ID as MOA-ID for the current application context. Sectoral Identity Management (MOA-ID) is extended to be transformed to Single Sign-On-capable. In this paper we are introducing the efficient result generation on Single-Sign-On Solution. This technique can be worked in piloting phase. No server issues were faced in this phase. To increasing the security considerations in resources is the main advantage of our requirement. We are developing above requirement in resolution management system. The incorporation of gained experiences of this piloting phase and the integration of our solution in further productive applications.

VII. REFERENCES

[1] T. Zefferer and T. Knall, "An Electronic-signature Based Circular Resolution Database Management System", In: Proceedings of the 25th Annual ACM Symposium on Applied Computing, 2010, pp. 1840-1845.

[2] Bernd Zwattendorfer, Arne Tauber, Thomas Zefferer," A Privacy-Preserving eID based Single Sign-On Solution", 978-1-4577-0460-4/11/$26.00 ©2011 IEEE

[3] H. Leitold, A. Hollosi, and R. Posch, "Security Architecture of the Austrian Citizen Card Concept" in Proceedings of the 18th Annual Computer Security Applications Conference (ACSAC '02).

[4] H. Lockhart and T. Hardjono, "SAML V2.0 Holder-of-Key Web Browser SSO Profile Version 1.0", OASIS, August 2010.

[5] Sharon E. Perl, Margo Seltzer," Data Management for Internet-Scale Single-Sign-On", Proceedings of the twelfth ACM symposium on Operating systems principles (New York, NY, USA, 1989), ACM Press, pp. 202–210.