Proxy Authenticator - Approach of a Signature based Single Sign On Solution for e-Government Services

Klaus John, Stefan Taber, Andreas Ehringfeld
Vienna University of Technology Research Group for Industrial Software (INSO)
Wiedner Hauptstraße 76, Stiege 2, 2. Stock
1040 Wien, Austria
klaus.john@inso.tuwien.ac.at
stefan.taber@inso.tuwien.ac.at
andreas.ehringfeld@inso.tuwien.ac.at

Abstract: This paper illustrates the development of an e-government solution for an application of a single-sign-on technology without the use of the SAML V2.0 protocol. We were confronted with the task of creating and implementing this kind of secure system, running on myHelp.gv.at, which is one of the Austrian e-Government Portals. The solution – or as we call it 'proxy authenticator' – enables us to omit any alterations to existing protocol structures or to amend the software architecture for all Austrian e-government applications.

1 Introduction

In recent years, the use of Information and Communication Technology (ICT) in administrative procedures (e-government) has gained much attention in efforts to modernise government in the European Union. Within the framework of the STORK1 [S013] EU project an electronic e-delivery service has been implemented for the Austrian e-government.

This paper describes the Austrian SSO solution for authentification against e-delivery services (proxy authenticator). For security purposes it does not store the private key in the citizen´s client browser but in a trusted centralised authority service, called myHelp.

2 Architecture of the Proxy Authenticator

The solution of a signature based proxy authenticator for e-government services requires user friendliness, a strong secure architecture and compliance with Austrian Law (§35 ZustG) [AG82]. SAML V 2.0 conflicts with the law concerning identification and authentication has to be done using the Austrian citizen card or by a special agreement using a secure technology called "automated triggered signature".

The architecture can be divided into three domains: citizen (Private User Domain), provider (myHelp Domain) and e-delivery services (Service Domain). These three domains are displayed in figure 1.

From the citizens' perspective the user logs into a e-delivery service where she/he generates a certificate and private key, which enables them to download documents from the service. The certificate and private key are uploaded into myHelp portal. The citizen can register multiple different e-delivery services. Afterwards one can use help.gv.at as a single sign on portal and gain access to all registered e-delivery services. After the authentication using the citizen card and an additional automatic login into the e-delivery service, the service will be passed on and executed without any user interaction. There is no legal relationship between the two – whereas the myHelp portal functions as a proxy service, the e-delivery service operates as an e-government service that transfers documents between citizens and government administration.

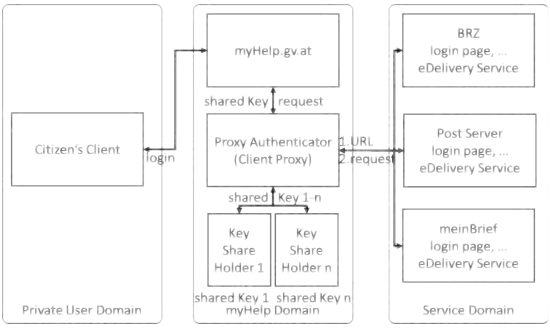

Figure 1: Proxy Authenticator Architecture

The myHelp Domain includes myHelp, a/the proxy authenticator and the key share holders. Between these components and the other domains only SSL connections are implemented. The private key is distributed amongst the key share holders, each of whom allocates a share of the key (e.g. by using cryptogaphical concept of Shamir´s Secret Sharing [S79]). Only the proxy authenticator can reconstruct the key to encrypt and decrypt the uploaded certificate and private key of the citizen.

3 Conclusion

This solution fullfills the security requirments, saves time, effort, and costs, by connecting all required e-government services into an existing e-governemnt portal through the proxy authenticator without changing any source codes.

References

[S79] Shamir, Adi (1979): How to share a secret. In: Communications of the ACM 22 (11): 612–613

[S013] STORK: Secure electronic identity across Europe; home page, Link:https://www.eid-stork.eu/pilots/index.htm; 24.03.2013

[AG82] Austrian Government (no Date): Bundesgesetz über die Zustellung behördlicher Dokumente (Zustellgesetz - ZustG), StF: BGBl. Nr. 200/1982 (NR: GP XV RV 162 AB 1050 S. 110. BR: S. 421.) §35 Ab. 1 bis Abs. 9