Design Shortcomings in E-Service Enrolment Processes: Recommendations From an HCI Perspective

Chris Porter, Faculty of Information and Communication Technology, University of Malta, Msida, Malta

ABSTRACT

Enrolment processes could make or break the success of an e-government service, and bad design decisions could build up to a catastrophic failure in e-service take-up. This article reviews a number of public-sector and commercial services which experienced adoption issues (or successes) arising from enrolment-related design decisions. A set of design shortcomings was synthesised, drawing on literature to assess their impact on end users, as well as on the service provider. These design shortcomings, along with a set of actionable recommendations, are discussed and presented with respect to the user, the task at hand and the environment of use, thus aligning this discussion to the core pillars of ISO-9241-210 (Ergonomics of human-system interaction – Part 210: Human-centred design for interactive systems).

KEYWORDS

Design, Enrolment, E-Services, Human-Computer Interaction, Onboarding, Workload

INTRODUCTION

E-services, as part of a transformational e-government strategy, are put in place to motivate citizen interaction with government in a cost-effective, convenient and accessible ecosystem. Badly designed e-services may impede this and could, in turn, damage the strategy along with the policy-maker’s goodwill. Identity-related processes, including enrolment, authentication and credential recovery are put in place to enable safe and secure interaction between the parties involved, safeguarding assets and well-being. However, such processes could also become hurdles for citizen adoption, negatively affecting the return on investment especially for public facing transactional e-services. Different services require different levels of identity assurance, and enrolment processes are put in place to deliver them. From the citizens’ perspective, these processes often require an amount of effort that exceeds the level of perceived risk, and benefits associated with the respective e-service. The perceived lack of proportion causes friction and is one of the root causes for low e-service take-up. Sasse and Fléchais (2005) argue that, in reality, security mechanisms are chosen without considering the production task and its performance requirements.

The focus of this paper is shortcomings in enrolment processes and related design decisions, while discussing possible approaches to overcome them. A human-computer interaction (HCI)
perspective will be taken, basing the discussion on three principal aspects of human-centred design for interactive systems, as adopted in ISO-9241-210 (ISO, 2008), namely: the user; the task at hand; and the environment of use. Understanding the context of use, which entails the user, the task at hand, and the time, place and conditions in which the task will be performed, is as important as getting the requirements, (including security requirements) right.

The various observations presented and discussed in this paper are based on a systematic review of relevant literature. The text corpus included official statistics, government publications, as well as results published by academic bodies. Therefore, research provides the contribution to knowledge by synthesising and discussing six enrolment-related shortcomings related to public-sector e-service design, while also providing a series of practical recommendations to overcome them.

Paper is organised as follows. An overview of the domain is first given, providing the necessary background upon which the rest of the paper builds. Following the aim and methodology sections, this paper then provides evidence, both experiential and empirical, on the effects that enrolment-related design decisions can have on e-services and users alike. Finally, a series of six design shortcomings are synthesised from the review, and are furthermore substantiated with practical recommendations. The paper then concludes by summing up the main take-aways from this discussion.

BACKGROUND

Enrolment refers to the set of actions a user needs to perform before being granted access to an e-service. This involves the verification of the user’s identity, as well as the generation of credentials (and shared secrets) to be used for authentication purposes in future interactions. This generally requires a user to provide the necessary proof of identity – the level of proof required by a service provider (identity assurance) depends on the risk levels involved (see Table 1). In low-assurance-level scenarios users may enroll by simply providing a valid e-mail address. However, when assurance-level requirements increase, more proof of identity may be required. In high-assurance-level scenarios, users may also be required to visit an enrolment centre in person to present other forms of identity (e.g. driver’s licence and biometric data). The term ‘enrolment process’ will be used as an umbrella term to represent other commonly used terms, including ‘signing up’ and ‘registration process’.

Establishing a proportional level of identity assurance for any given e-service could be a challenging task, primarily in avoiding introducing over-zealous levels of security that may have a negative impact on user adoption or onboarding. Imposing identity-assurance level requirements for an e-service without proper consideration for the users’ experience may come at a cost, and evidence for this is presented in two upcoming sections: Evidence from the Field and Evidence from Literature. Nonetheless, risk levels pertaining to an e-service should also be respected, and there are circumstances where a high level of identity assurance would be necessary. Finding the right identity mechanism to deliver such assurance, while taking into account user capabilities, perceptions, expectations, as well as limitations and opportunities afforded by the context, is a non-trivial problem.

Beaumont et al. (2008) introduce what the authors refer to as the ‘compliance budget’, which is as an organisational technique to understand, manage and potentially influence user behaviour when introducing security policies within an organisation. While studying employee security behaviour at two major commercial organisations, the authors noticed that the employees’ perception of costs and benefits of complying with organisational security requirements had a direct influence on behaviour – which could ultimately have had a major impact on the effectiveness of the company’s overall security goals. There was a limit on the effort individuals are ready to make (perceived costs) to comply with organisational security requirements. However, the higher the perceived benefits, the better the chances that users would comply. If the amount of perceived effort required from the user is higher than the individual’s level of perceived benefits (compliance threshold) there is a higher risk that the user would not comply with the required security measure(s) – unless compulsion exists. This could also result in disruption, frustration, and possibly failure to complete the task at hand.
Understanding the Impact of Wireless Local Area Networks on Users and Assessing User Satisfaction with Wireless Local Area Networks

Car Navigation System using Genetic Algorithm Processor
Masaya Yoshikawa (2011). Service Intelligence and Service Science: Evolutionary Technologies and Challenges (pp. 216-226). www.igi-global.com/chapter/car-navigation-system-using-genetic/47363?camid=4v1a