Identification Now and in the Future: Social Grant Distribution Process in South Africa

Stephen Flowerday and Gideon Ranga
Information Systems Department, University of Fort Hare,
P. O. Box 7426, East London, 5200, South Africa.
sflowerday@ufh.ac.za; rangags@gmail.com

Abstract. This paper seeks to apply Identity Management (IDM) principles to the social grant distribution process in South Africa, which has been prone to fraud and corruption. It discusses the social grant distribution process and the problems encountered. Suggested solutions to the problems are highlighted and these include moving from an Isolated IDM architecture to either a Federated and/or Centralised IDM architecture.

1 Introduction

The government of South Africa, under the Ministry of Social Development, has formed the South African Social Security Agency (SASSA) which is responsible for the distribution of social grants to ten million underprivileged citizens. Of the three billion Rand invested in social grants per month, more than five percent is lost to fraud [1]. Much of the fraud is attributed to Identity Management problems. This paper begins by discussing the social grant distribution process in South Africa. It then states the problems experienced in the process. Finally, the paper discusses how the process could function in the future so as to minimise the fraud caused by the Identity Management problems.

2 Social grant distribution process

SASSA subcontracts the issuing of social grants to distribution companies which carry out the identification and the verification processes in different parts of the country. SASSA and the distribution companies obtain a list of eligible recipients from local government and enrol the beneficiaries onto the system. The distribution companies identify and verify a social grant beneficiary using biometrics and smart cards and then issue the grant to the eligible recipient [2]. The process involves

checking an individual's fingerprints against templates in a local database and verifying it against a template encoded onto a smart card. The social grant distribution process is an IDM system in that it seeks to allow certain rights (in this case social grants) to certain people (users) and currently adopts an Isolated IDM architecture [2].

3 Problems associated with the social grant distribution process

The following points are identified as problems encountered during the social grant distribution process.

1. Since the templates are tested in local databases, there have been cases where people have more than one smart card and a fake ID number, which allows them to obtain grants at different locations. Presently there is no central database which verifies all the fingerprints that are existent in order to detect duplicity [3].
2. Most of the beneficiaries are in rural areas and this introduces additional challenges in that many rural areas are outside the telecommunications and electrical grid. This results in the transactions being conducted offline rather than in real-time where automatic updating of databases occur. Updating of data therefore takes place at night and often occurs more than twenty-four hours after the transactions have been performed. This results in fraud occurring within this twenty-four hour window period [3].
3. There are cases whereby different people may erroneously have the same ID number and this complicates the enrolment stage because the recipients may all be eligible to receive the grant yet the system identifies them as one entity and therefore pays out only once [4].
4. Another problem identified is the use of fingerprints in the enrolment process. As people age their fingerprints are no longer clearly defined due to the nature of the work many of the people participate in, especially in the rural areas [2].
5. Finally, when people travel they are required to go back to their districts where they originally registered because the system does not allow an individual to receive a grant at different locations. This causes inconvenience including the cost implications of returning to the original district in order to receive one's grant [3].

4 Suggested solutions and conclusion

There should be a federation between the various distribution companies and databases of different geographical locations. This will enable users to sign in wherever they are and monitoring between the companies will become more effective. The system should consider incorporating a Federated Identity Management (FIDM) model which manages identities across policy and/or

application domains in which the identity data is distributed [6, 7]. In addition it should ensure that there is proper authentication and authorisation of individuals in order to address points 1, 3 and 5 [5]. As SASSA is one organisation it could consider incorporating a centralised model for easy administration and audit. Furthermore a Centralised IDM model has strong Single Sign-On (SSO) capabilities which enables users access to their resources (grants) anywhere which assists with point 5 [8]. IDM solutions and architectures however will fail to solve point 2 because this is a rural development and telecommunications problem and not necessarily an IDM issue. Additionally biometric mechanisms such as face, voice and iris recognition could be used as an alternative to the fingerprint method in cases where this method does not suffice in order to address point 4 [9]. The central database however has its own security, privacy, cost implications and administrative risks.

References

1. InfoSA. (2005). About South Africa, 2005. Available from :<http://www. southafrica. info/ess_info/sa_glance/social_delivery/social_grants.htm> [Accessed: 15 August 2006].
2. Rusere, L. (2006). AllPay Social Grant Distribution Company. East London, South Africa.
3. de Jongh, A. (2006). AllPay Distribution Company. East London, South Africa
4. Macocozoma, B. (2006). Deal House Social Grant Distribution Company. East London, South Africa.
5. Fidis, (2006). ID-related Crime: Towards a Common Ground for Interdisciplinary Research. *Future of Identity in the Information Society.* White Paper, fidis-wp5-del5-2b.ID-related.crime.doc.
6. Madsen, P. Koga, Y. & Takahashi, K. (2005). Federated Identity Management For Protecting Users from ID Theft. *Computer-Communications Networks.*
7. Ahn, G. & Lam, J. (2005). Managing Privacy for Federated Identity Management. *Communications of ACM.*
8. Josang, A. Fabre, J. Hay, B. Dalziel, J. & Pope, S. (2004). Trust Requirements in Identity Management. *Distributed Systems Technology*.
9. Wayman, J. (2000). Picking the best Biometric Authentication Technologies. *National Biometric Test Center Collected Works.* vol. 1, pg, 269-275.