An Hybrid User Identity Model to Electronic Identities Management

José Alberto Sousa Torres[1,2], Rafael Timóteo de Sousa Júnior[1]
University of Brasilia[1], Brazilian Ministry of Justice[2]

Universidade de Brasília

INTRODUCTION

Identity theft is one of the biggest barriers to spread the use of online transactions, such as those that are used in the electronic government. To reduce the occurrence of identity theft, governments and private companies need to adopt a reliable way to electronically identify people.

Further more, in order to improve the adoption of the authentication system, governments need to provide methods to preserve their privacy and to protect the citizen´s personal data. The key challenge for countries in the definition of their identity management strategies is to find the right balance between privacy and fraud prevention.

Recently, the Brazilian government launched the process of creating their unique national identity. The government defined four main requirements to develop its strategy in order to maintain the correct threshold between privacy and control:

- The electronic identity should be used to identify people in transactions with public agencies and private companies
- The financial sustainability of the system must be guaranteed by charging transactions with private companies.
- Citizens should see just "one government" and government should see just "one citizen".
- The user privacy should be preserved.

Unfortunately, there is not in the literature a model that fully address all these requirements. Four main types of identity management models are defined : silo-based, centralized, federated and user-centric. Commonly, countries adopt

PROPOSAL

Our proposal is to define an hybrid identity model that allows frauds prevention at the same time that trying to preserve the user private life. Differently than do most countries, which treats in the same way all user transactions, the proposed model separates these transactions into two different groups: those transactions which are related to identify users with public agencies; and those related to identify users with private companies.

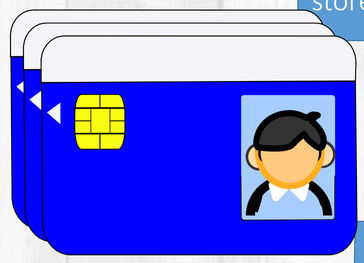
The main idea is to use different identity models for different transaction groups. Thus, the centralized model - which is the optimal model for fraud prevention, would be used for transactions with the public sector, while the user-centric model, which is the best model for ensuring privacy, would become the basis for users could interact with private sector.

This approach is optimal in the context of treat the whole government as a single entity, considering that data stored in a public agency could be shared with others to improve the quality of public service provision. At the same time, the use of user-centric operations with private entities would prevent that the government could track every step of the user, knowing everything about he do in his private life.

Hybrid User Identity Model

The government individualizes citizens and stores the personal data on a centralized database

The government issues an electronic credential that locally stores the personal data of users



gov.br

Centralized Model
"More Control"
"Less Privacy"

- The user credentials are checked online in a centralized environment to electronic government transactions.
- All users interactions with the government services are logged.
- The citizen´s data and interactions are shared among public agencies.
- Citizens see just "one government ".
- Government see just "one citizen"
- Government can use the shared data to implement ways to reduce frauds.
- Government can not share citizen data with private companies
- Government should not access the log of the user transactions with private companies.

User-Centric Model
"Less Control"
"More Privacy"

- Private companies check the user credentials locally through a match-on-card operation.
- Government provide a way to authenticate users (citizen card) but do not log the citizens private transaction.
- The main question is to find a way to bill offline transactions. This can be solved in three different forms:
  - Users need to add "transactions credit" to the citizen card to enable the execution of the match-on-card transaction.
  - Government provides a middleware to the card-reader machines that works just when there is "transaction credits" charged in the machine. This credit should be acquired by the companies and loaded in the readers.
  - It can be used a protocol to provide centralized and remote anonymous authentication with the possibility to bill the transactions (work in progress).

Conclusions and Work in progress

- A drawback of this approach is that the governments need to spend money twice to implement the solution, one of them to keep the central online database the other to issue the technologic identity cards.
- One of the main challenge of these hybrid approach is to permit to the government to charge the provision of authentication services in a user-centric authentication model, i.e., how the government can charge an offline authentication service and how governments can provide authentication without make a record of all user actions.
- We are currently working in three approaches to solve this problem, one alternative is charge the users using the same logic used in the pre paid debit cards, so users would need to put transaction credits in theirs electronic identity cards before try to execute an authentication transaction. The second alternative is to introduce charges to companies through the purchase of transactions credits that will be loaded into the middleware of the card readers. In both ways the government can provide the authentication service and to bill the transaction without log the users steps. We are also studying a protocol that allows centralized authentication through the use of pseudonyms.

ECEG 2015

Posters

acpi

University of Portsmouth

University of Portsmouth

Proceedings of the 15th European Conference on e-Government

University of Portsmouth, UK

18-19 June 2015

Edited by

Carl Adams
University of Portsmouth, UK

acpi

A conference managed by ACPI, UK

Proceedings of
The 15th European Conference on eGovernment

ECEG 2015

University of Portsmouth
UK

18-19 June 2015

Edited by
Dr Carl Adams
University of Portsmouth
UK

Papers submitted to this conference have been double-blind peer reviewed before final acceptance to the conference. Initially, paper abstracts were read and selected by the conference panel for submission as possible papers for the conference. Many thanks to the reviewers who helped ensure the quality of the full papers.

Conference Proceedings

The Conference Proceedings is a book published with an ISBN and ISSN. The proceedings have been submitted to a number of accreditation, citation and indexing bodies including Thomson ISI Web of Science and Elsevier Scopus for indexing.

The Electronic version of the Conference Proceedings is available to download from **DROPBOX**. (**http://tinyurl.com/ECEG2015**) Select Download and then Direct Download to access the Pdf file. Free download is available for conference participants for a period of 2 weeks after the conference.

The Conference Proceedings for this year and previous years can be purchased from http://academic-bookshop.com

E-Book ISBN: 978-1-910810-20-0
E-Book ISSN: 2049-1034
Book version ISBN: 978-1-910810-19-4
Book Version ISSN: 2049-1026
CD Version ISBN: 978-1-910810-21-7
CD Version ISSN: 2049-1042

Published by Academic Conferences and Publishing International Limited
Reading, UK
44-118-972-4148
www.academic-publishing.org