

Accepted Manuscript

Privacy-preserving attribute aggregation in eID federations

Walter Priesnitz Filho, Carlos Ribeiro, Thomas Zefferer

PII: S0167-739X(17)32796-6
DOI: <https://doi.org/10.1016/j.future.2018.09.025>
Reference: FUTURE 4460

To appear in: *Future Generation Computer Systems*

Received date : 21 December 2017
Revised date : 21 July 2018
Accepted date : 9 September 2018

Please cite this article as: W. Priesnitz Filho, et al., Privacy-preserving attribute aggregation in eID federations, *Future Generation Computer Systems* (2018), <https://doi.org/10.1016/j.future.2018.09.025>

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.



Privacy-preserving Attribute Aggregation in eID Federations

Walter Priesnitz Filho^{a,*}, Carlos Ribeiro^{a,1}, Thomas Zefferer^{b,1}

^a*Instituto Superior Técnico, Universidade de Lisboa
Av. Rovisco Pais, 1, 1049-001 Lisboa, Portugal*

^b*Secure Information Technology Center Austria
Inffeldgasse 16a, 8010 Graz, Austria*

Abstract

Personalized electronic services, e.g. from the e-government domain, need to reliably identify and authenticate users. During user-authentication processes, the electronic identity of the respective user is determined and required additional attributes, e.g. name and date of birth, linked to this identity are collected. This attribute-collection process can become complex, especially if required attributes are distributed over various attribute providers that are organized in a federated identity-management system. In many cases, these identity management systems rely on different ontologies and make use of different languages. Hence, identity federations, such as the one currently established across the European Union, require effective solutions to collect user attributes from different heterogeneous sources and aggregate them to a holistic user facet. At the same time, these solutions need to comply with minimum disclosure rules to preserve users' privacy. In this article, we propose and introduce a solution for privacy-preserving attribute aggregation. Our solution combines attributes from different domains using ontology alignment and makes use of locality sensitive hashing functions to preserve users' privacy. Evaluation results obtained from conducted experiments demonstrate our solution's advantages for both, service providers and users. While service providers can be provided with a larger set of attributes, users remain in full control of their data and can decide on which of their attributes shall be revealed.

Keywords: Electronic identity, Identity federation, Attribute aggregation, Interoperability, Ontologies, Privacy

1. Introduction

Governments and public administrations face the challenge to continuously improve their e-government infrastructures in order to cope with fast-changing requirements and to provide citizens useful electronic

*Corresponding author

Present address: Universidade Federal de Santa Maria - Av. Roraima, 1000 Prédio 5 97105-900 Santa Maria - RS, Brasil

Email addresses: walter.filho@tecnico.ulisboa.pt (Walter Priesnitz Filho), carlos.ribeiro@tecnico.ulisboa.pt (Carlos Ribeiro), thomas.zefferer@sit.at (Thomas Zefferer)

Download English Version:

<https://daneshyari.com/en/article/11012467>

Download Persian Version:

<https://daneshyari.com/article/11012467>

[Daneshyari.com](https://daneshyari.com)