Accepted Manuscript

Title: Fast revocation of attribute-based credentials for both users and verifiers

Author: Wouter Lueks, Gergely Alpár, Jaap-Henk Hoepman, Pim Vullers

PII: S0167-4048(16)30172-9
DOI: http://dx.doi.org/doi: 10.1016/j.cose.2016.11.018
Reference: COSE 1073

To appear in: *Computers & Security*

Please cite this article as: Wouter Lueks, Gergely Alpár, Jaap-Henk Hoepman, Pim Vullers, Fast revocation of attribute-based credentials for both users and verifiers, *Computers & Security* (2016), http://dx.doi.org/doi: 10.1016/j.cose.2016.11.018.

Fast Revocation of Attribute-Based Credentials for Both Users and Verifiers*

Wouter Lueks[1], Gergely Alpár[12], Jaap-Henk Hoepman[1], Pim Vullers[1]

[1] Digital Security, Institute for Computing and Information Sciences, Radboud University, Toernooiveld 212, Nijmegen, The Netherlands

{lueks, gergely, jhh, pim}@cs.ru.nl

[2] Faculty of Management, Science & Technology, Open University of the Netherlands, Valkenburgerweg 177, Heerlen, The Netherlands

Wouter Lueks is a PhD student at the Radboud University in Nijmegen, The Netherlands. He works on privacy-enhancing technologies, and he is in particular interested in creating systems that offer anonymity, while at the same time are capable of resisting abuse. He graduated in 2011 from the University of Groningen, receiving master's degrees in Mathematics and Computer Science, both with distinction.

Gergely AlpÃ¡r PhD is a University lecturer at the Open University (Netherlands) and visiting researcher at Radboud University in computer science. His main research interest is cryptography, attribute-based identity management and mathematics teaching. He holds a master's degree in mathematics and education, and a Professional Doctorate in Engineering in applied mathematics. Gergely is an external member of the Privacy & Identity Lab where, besides interdisciplinary discussions, he organised the first international attribute-based credential workshop. Currently, he also works on developing a new kind of university mathematics teaching method in cooperation with the Stanford University.

Jaap-Henk Hoepman (1966) is associate professor at the Digital Security group of the Radboud University, Nijmegen, the Netherlands. He is also scientific director and co-founder of the Privacy & Identity Lab. He studies privacy by design and privacy friendly protocols for identity management and the Internet of Things. He speaks on these topics at national and international congresses and publishes papers in (inter)national journals. He also appears in the media as security and privacy expert, and writes about his research in the popular press. He is actively involved in the public debate concerning security and privacy in our society.

Pim Vullers joined the Digital Security group at the Radboud University in Nijmegen in 2009 after receiving his MSc degree in Computer Science and Engineering from the Eindhoven University of Technology. He has been working on privacy-enhancing technologies in general and attribute-based credentials in particular. The main focus of his research has been on efficient implementations for smart cards, resulting in a PhD degree in 2014. After graduating he joined NXP Semiconductors as a software security engineer.