Publicly Accountable Privacy Revocation

Joakim Brorsson[1,2] and Paul Stankovski Wagner[1]

[1] Department of Electrical and Information Technology, Lund University, Sweden
{joakim.brorsson, paul.stankovski}@eit.lth.se
[2] Combitech AB, Växjö, Sweden

Abstract. This paper introduces the notion of *Publicly Accountable Privacy Revocation* (PAPR). An identification scheme with this property provides both conditional privacy of users and public verifiability of correct behavior of privacy revocation authorities. That is, users retain full privacy when authenticating to third parties and authorities have the capability to revoke this privacy retroactively, but in doing so they necessarily make the public aware of this action.
We further describe how to construct a pseudonymous credential system with the PAPR property. The described system specifies a privacy revocation procedure that requires the participation of a specific set of users which are not known to the authority in advance. Public accountability is thereby achieved since the authority has to issue a public query in order to find these users.

1 Introduction

The trade-off between privacy and security has gained interest in the cryptographic research community, both from a technical perspective in academic research, and from an ethical perspective in reports and open letters. In order to loosen this knot of seemingly opposing sides in the trade-off, we here provide a tool for auditing authorities with surveillance capabilities, in the context of privacy preserving authentication. Our insight is that in today's systems, there is no accountability towards the public for authorities which have the power to revoke privacy from users. We therefore aim to relax the tension in the trade-off by imposing measures which provide public verifiability that authorities follow the rules they are bound to, i.e., we introduce accountability and transparency for these authorities. These measures can enable an increased (user) trust in a system, and the presented construction may also serve as a basis for discussion on the use of privacy revocation powers.