Chapter 9
Technical Implementation and Feasibility

Gert Læssøe Mikkelsen, Kasper Damgård, Hans Guldager, Jonas Lindstrøm Jensen, Jesus Garcia Luna, Janus Dam Nielsen, Pascal Paillier, Giancarlo Pellegrino, Michael Bladt Stausholm, Neeraj Suri, and Heng Zhang

Abstract This chapter provides application developers with a presentation of the implemented reference implementation of the ABC4Trust architecture and protocols as well as a presentation on how to get started using the reference implementation. The reference implementation includes the ABC-Engines of the different entities, namely the User, Issuer, Verifier, Inspector, and Revocation Authority, and the smart card implementation for the User. This chapter also presents results of a perturbation analysis of the reference implementation. Even though the ABC4Trust focused on a server-desktop environment, we have done some proof of concept implementations and analysis of the feasibility of using smart phones for the user side of a Privacy-ABC setup; these results are also presented in this chapter.

This chapter will give an introduction and an overview of the reference implementation, including an introduction to a number of issues related to the reference implementation. It will however, not necessarily be exhaustive, i.e., in most of the cases further reading is required to get a complete understanding of the issue at hand. The presentation will start of by giving an explanation of the source code itself. This includes instructions on how to obtain and build the reference implementation, how

Gert Læssøe Mikkelsen, Kasper Damgård, Jonas Lindstrøm Jensen, Janus Dam Nielsen, and Michael Bladt Stausholm
Alexandra Institute, Aabogade 34, DK8200 Aarhus N., e-mail: {gert.l.mikkelsen, kasper.damgaard, jonas.l.jensen, janus.nielsen, michael.stausholm}@alexandra.dk

Hans Guldager
Miracle A/S, Skanderborgvej 232, DK8260 Viby J, e-mail: hgk@miracle.dk

Neeraj Suri, Jesus Garcia Luna, Giancarlo Pellegrino, and Heng Zhang
TU Darmstadt, Hochschulstraße 10, D-64289 Darmstadt, e-mail: suri@cs.tu-darmstadt.de, {jluna, gpellegrino, zhang}@deeds.informatik.tu-darmstadt.de

Pascal Paillier
Crypto Experts, 41 Boulevard des Capucines, 75002 Paris, e-mail: pascal.paillier@cryptoexperts.com

Springer International Publishing Switzerland 2015
K. Rannenberg et al. (eds.), Attribute-based Credentials for Trust, DOI 10.1007/978-3-319-14439-9_9
9.1 The Reference Implementation

In the ABC4Trust project a reference implementation [BBE+14] of a Privacy-ABC scheme has been implemented realizing the architecture demonstrated in Figure 9.1 and described in Chapter 2. The reference implementation has been used in the pilots of the ABC4Trust project, and has been made public available for others to use, as described in the next section. The reader is also referred to [BBE+14] for a description of the final reference implementation of the ABC4Trust project.