Appendix A: Direct Anonymous Attestation

A few solutions are focused on integrating DAA in existing trusted platforms, like ARM TrustZone, supporting security-critical services in microprocessor platforms. TrustZone, in particular, provides a secure area in the main processor, the Trusted Execution Enviroment (TEE), guaranteeing that the code and data loaded inside that area are protected: when a user invokes a secure operation, the system switches from the normal environment, called Rich Execution Environment (REE), to TEE. While TrustZone does not support the DAA in itself, a few DAA proposals for mobile devices are built on top ot its architecture. Wachsmann et al [**?**] propose a lightweight anonymous authentication scheme without linkability for embedded device exploiting TrustZone primitives. In [**?**] Zhang et al. proposed *Mdaak*, a DAA framework for mobile platform and, similarly, Yang et al. [**?**] propose a detailed infrastructure for four ECC-based DAA implementations. Nevertheless, neither work provides any protection mechanism for DAA data and, further, the overhead introduced by TrustZone TEE/REE context switching is ignored.

In [**?**] a DAA scheme based on TrustZone functionalities is realized. Additionally, this solution relies on SRAM PUF as a root of trust, considers the pre-computation of heavier setup values in order to realize a quite expensive execution, and further reduces the context switch overhead between TEE and REE. In addition to the previous proposals, the technical literature offers several comparisons among dif-

ferent DAA schemes useful to identify the best DAA scheme choice for a specific infrastructure and domain [**?**, **?**].