PRISEC2: Comparison and Use of Algorithms for Constrained Devices

Proposta de Projeto

Orientador: Paul Crocker (DI/UBI)
Co-Orientador: Valderi Leithardt (DI/UBI)

1 Objetivos

To conduct a feasibility study and analysis of the efficiency of several new and promising hashing algorithms and authenticated encryption within the context of the PRISEC (*) module of the UbiPri (Ubiquitous Privacy) middleware. The hash algorithms to consider are the BLAKE3 and Balloon Hashing algorithms amongst others and the encryption algorithms are Ascon and ACORN.The performance of the algorithms is to be analysed over several differnet architectures as well as differing programming languages.The algorithms should be integrated with the UbiPri middleware module.

(*) See for instance PRISEC: Comparison of Symmetric Key Algorithms for IoT Device https://www.mdpi.com/1424-8220/19/19/4312

2 Tarefas a Realizar

T1 Study of Hashing and Authenticated Encryption Algorithms (0.5M
T2 Implementation. (1M)
T3 Integration with the UbiPri middleware (1M)
T4 Project Report write up. (0.5M)

3 Requisitos Técnicos/Académicos

Programming Skills. Computer and Data Security. Concepts in Number Theory and Statistics.

4 Contactos

Paul Crocker (crocker@di.ubi.pt