Master Thesis – Towards Cryptographically Agile Applications

Motivation
- Cryptographic agility [1] describes the ability to evolve or repair hardware, software, or entire IT systems in an easy way [2].
- The rise of strong quantum computers [3] makes this even more important.

Goals
- Goal of this thesis is to provide typical measures to make applications and IT systems cryptographically agile.

Tasks
- Research various measures to provide cryptographic agility within applications, IT systems and hardware.
- Create a set of mandatory requirements that have to be fulfilled in order to make an application cryptographically agile.
- Define a methodology/process in order to transform an existing application into a more agile instance of this application.
- Evaluate the methodology/process in a prototypical manner including a small usability study.

Prerequisites
- Good knowledge in IT-security, cryptography & network protocols.
- Very good knowledge in software design.
- Good knowledge of usability.
- Independent and structured way of working.
- Knowledge of post quantum cryptography beneficial.
- Thesis language can be English or German.

Literature

Interested? Please contact us via email or personal.

Contact
Prof. Dr. Andreas Heinemann
andreas.heinemann@h-da.de

Alexander Zeier, M. Sc.
alexander.zeier@h-da.de

Website
https://ucs.fbi.h-da.de

Schöfferstr. 10
64285 Darmstadt