

A Secure Smart Element for Small Devices

Motivation

Modern small digital devices, or “gadgets”, demand secure storage and processing capabilities.

Modern flash storage solutions are small and portable, and storage should be encrypted in the case of loss or theft.

Not long ago the first Mobile Security Cards were introduced, which combine the functions of a smartcard with gigabytes of flash storage into one single card of microSD formfactor.

Project Description

This project explores the potential of the newest generation of integrated microSD security cards.

Connected to the microSD expansion slot of a modern smartphone these cards can be used for privacy and security sensitive applications.

An applet on the smartcard should be able to validate the security properties of the platform host and only if they fit release the cryptographic key for accessing the flash bulk storage.



Deliverables

Source of developed prototype.

Written documentation of approach, use case and comparison with previous efforts.

Scope & Credits

The effort and credits of this project are scalable

Advisor / Contact

Martin Pirker (mpirker@iaik.tugraz.at)

Johannes Winter (jwinter@iaik.tugraz.at)