Secure Portable USB Data Storage

Marcel Kleja (2), Marek Laban (1,2), Viktor Fischer (3)

(1) Department of Electronics and Multimedia Communications,
Technical University of Kosice, Park Komenskeho 13,
04120 Kosice, Slovak Republic
(2) MICRONIC, Sliacska 2/C, 83102, Bratislava, Slovak Republic
(3) Univ. Lyon, UJM-Saint-Etienne, CNRS, Laboratoire Hubert Curien
UMR 5516, F-42023, Saint-Etienne, France

Abstract

USB flash drive, also called pen drive or USB stick is a popular means of data storage, back-up and transfer. Some cryptographically secure versions of the stick exist, but only few of them can be trusted (if any).

Secure Portable USB Data Storage device was developed as Demonstrator 2 in the framework of the European H2020 project HECTOR (Hardware Enabled CrypTO and Randomness). It is based on a flash based FPGA SoC - Microsemi SmartFusion2 - which features a 32-bit ARM based microcontroller. The device was developed and tested on the HECTOR evaluation platform, which constitutes a modular system and makes evaluation of device features easier by using existing data and control interfaces.

The talk describes developed device and the various challenges during the development process. One of the aims of the talk is also to show the exploitation of the HECTOR project outputs like physically unclonable function, true random number generator and authenticated encryption algorithm in a future commercial device.