Development of the device for trusted session: S-Terra SPDS-USB-01

Customer
S-Terra CSP is a Russian developer and manufacturer of network security solutions. The company's solutions for building virtual private networks (VPN) provide protection for firewall interactions, wireless and multiservice networks, as well as ensure the security of remote and mobile users.

Objective
Develop and prepare for launching into production a custom bootable medium (hereinafter CBM) SPDS-USB-01 (SPDS: TCM, Trusted Computing Module), which is a USB device and designed to build trusted computing modules.

SPDS-USB-01 should perform the following functions:

● Access to a cryptographic controller operating according to ISO-7816-3
● Access to the data medium via the USB Mass Storage Interface
● Control of access to the sections on the data medium depending on the password received
● The possibility of booting IBM PC-compatible computers from the device
● The speed of data transfer over USB which equals that of flash drives by global vendors

It is necessary to develop a library to provide the API programmer with control of the device via USB CCID in Linux. It is also necessary to develop a software package
executed on the controller and the PC, which would perform post-production testing and startup initialization of the device, involving the creation of passwords and rights, as well as the writing of operating system images to the device.

Solution

1. Hardware development

The software was based on the AT91LIB library by Atmel. The solution was designed using an ARM Cortex M3 chip.

![Fig.1. Structural diagram of the device](image1)

![Fig.2. A hardware platform of the device](image2)
2. Software development

Considering the customer’s requirements, the following software architecture was developed:

![Software architecture diagram](image)

Fig. 3. Software architecture

Major software modules:

1. USB CCID provides access to a smart card (smart chip) through the ISO7816 interface.
2. USB MSD provides access to the eMMC Flash content according to the rights of the user authorized through the USB CCID.
3. Login checks the responses of the smart card through the ISO7816 interface and, based on the response, issues the right of access to data in the MSD infrastructure.
The initialization of the device involved the use of the Debian 6.0 operating system, as well as the usblib and libsysfs libraries. Three libraries were created using these tools:

1. libinitsbs provides the functions of authorization and writing data to the device.
2. libsbs provides the functions of communication with a smart card (reset, creating a file system, adding a user, user authorization, deleting a user, blocking a user, etc.).
3. the libsysfsdev library.

Benefits

- The device operating principles are based on a fundamentally new technology that allows building a trusted session environment. It eliminates the costly and difficult to use security packages such as security suite, NAC, DLP, and others
- Data on the device are protected by a crypto chip (smart card): two-factor authentication, cryptographic protection of data and traffic
- The possibility of booting an operating system from the device
- The security products were certified in systems of FSTEC of Russia and Federal Security Service of Russia