As we have less and less time, the information interoperability becomes more and more important. The personal information environment plays a more and more important role in a person's life.

And we clearly know what do we want from the tools that provide the informational interoperability – it is **mobility, user-friendliness and protection**.

This is what we wish for.
And what do we get?

In real life, we become more connected to our computer, which performs the function of an interface between the person and his information environment.

As a result, we need to either limit our movement or carry PC with us everywhere, just in case we need something.

At the same time, it is quite obvious that the presence of a specific PC is not required in most of the situations. As a rule, a ***unique* personal information environment is formed by a relatively small volume of data and programs**.

That is why, to the detriment of the information protection, people often select a more mobile and friendly alternative – copying the data on various carriers and using it on other computers.
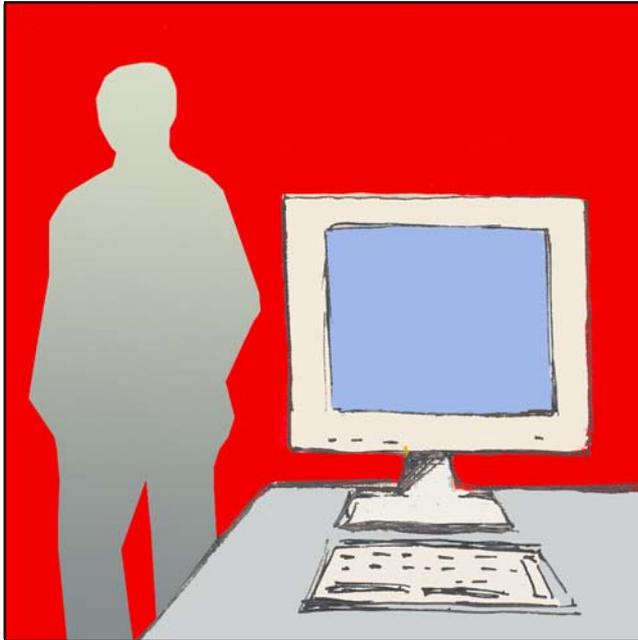
In order to protect yourself from the Unauthorized Access to this data, you can encrypt it, but to do that you need to at least trust the performance of the cryptographic transformation by one or another technical device.

If we are going to use such information protection methods as encryption and/or the Electronic Digital Signature on someone else's computer, it is necessary to copy the keys to some carrier in advance.

That means that in order to provide the protection of one data, we need to significantly decrease the safety of other data. To be more specific, it is exactly the data that the security of the first data depends on. We see a definite contradiction, which borders on absurdity.

Using different web-services, we are forced to either disregard the "safety rules", writing the passwords down on paper or into the unprotected files, risking to either mix up or forget them. Although, you can also strictly limit the number of the used web-services in accordance with how many passwords you are able to remember. It's doubtful that you will be able to remember a lot.

You need a secure passwords storage, which will not only be resistant to the unauthorized access, but will also prevent the user from getting mixed up in all of his passwords.

We cannot manage our banking account from someone else's computer, for example, using the software like "Client-Bank". In this case, it is not too smart to choose between the protectability and mobility. However, the need for a protected and mobile solution of this kind is obvious today.

The users that prefer licensed software pick quality over mobility. When using the Product Activation type technologies, the number of computers, which the software may be activated on, is limited.

The technology of hardware-based security, linking the software and the user, not the software and the computer, has grown form the understanding of this problem, which is fair – the person has paid for the licensed copy and is its owner.

However, the presently existing realizations of this technology, provide the mobility at the cost of protectability – emulating their operation is just as easy as entering a "unique" serial number or license key. Moreover, unfortunately, these hardware tools are often so poorly realized that using the "protected" product becomes impossible.

Choosing the lesser of two evils, neglecting some of the time requirements in favor of the other ones, becomes more and more complicated.

This means that it is now the time for a device, which will free the human being from the need to choose among the necessary.

It is a PERSONAL CRYPTOGRAPHIC INFORMATION PROTECTION TOOL.

PCIPT SHIPKA meets the requirements of our time, because it allows always carrying the necessary personal data with you, such as the keys and certificates, the user software and so on, and allows using all of this on any computer that has a USB-interface.

Moreover, it allows doing that with no threat to the information protection.

This is achieved by means of the **hardware implementation of the cryptographic algorithms, a hardware random-number generator, protected non-volatile memory and applying the keys the way that they never get transferred to PC.**

In order to use SHIPKA, you don't need any additional equipment or special skills or installing any cryptographic libraries on your computer.

The cryptographic library of SHIPKA provides the calculations by all Russian cryptographic algorithms:

· Encryption by **GOST 28147-89**,
· The hash-function calculation by **GOST R. 34.11-94**,
· Calculation and checking of the EDS by **GOST R. 34.10-94** and **GOST R. 34.10-2001**,
· Calculation and checking of the authentication protection codes (APC).

Beside that, SHIPKA offers all of the most widespread and popular foreign algorithms, such as:

· Encryption – **RC2**, **RC4** and **RC5**, **DES**, **3DES**, **RSA**,
· The hash-function calculation – **MD5** and **SHA-1**,
· Calculation and checking of the EDS – **RSA**, **DSA**.

<u>**The hardware implementation of the calculations**</u> without the involvement of the computer resources is a distinguishing feature of SHIPKA, compared to other known solutions on the basis of the USB-keys, which practically represent a non-volatile memory and a USB-interface adapter, while the critical level of the calculations is <u>software-based</u>.
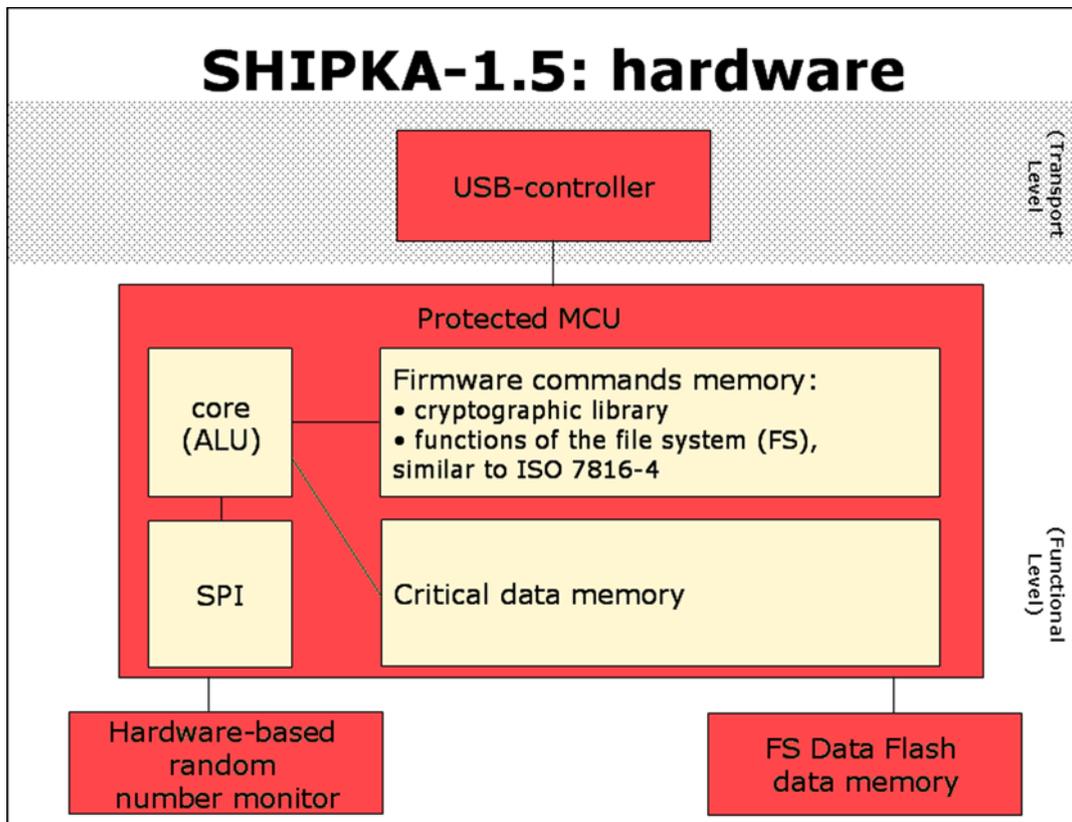
In SHIPKA, the only software-based procedures are the transport procedures and the data formats coordination procedures, which don't influence the security.

This means that no interference with the course of the authentication, encryption or production/checking of the Electronic Digital Signature processes is possible, same as their falsification.
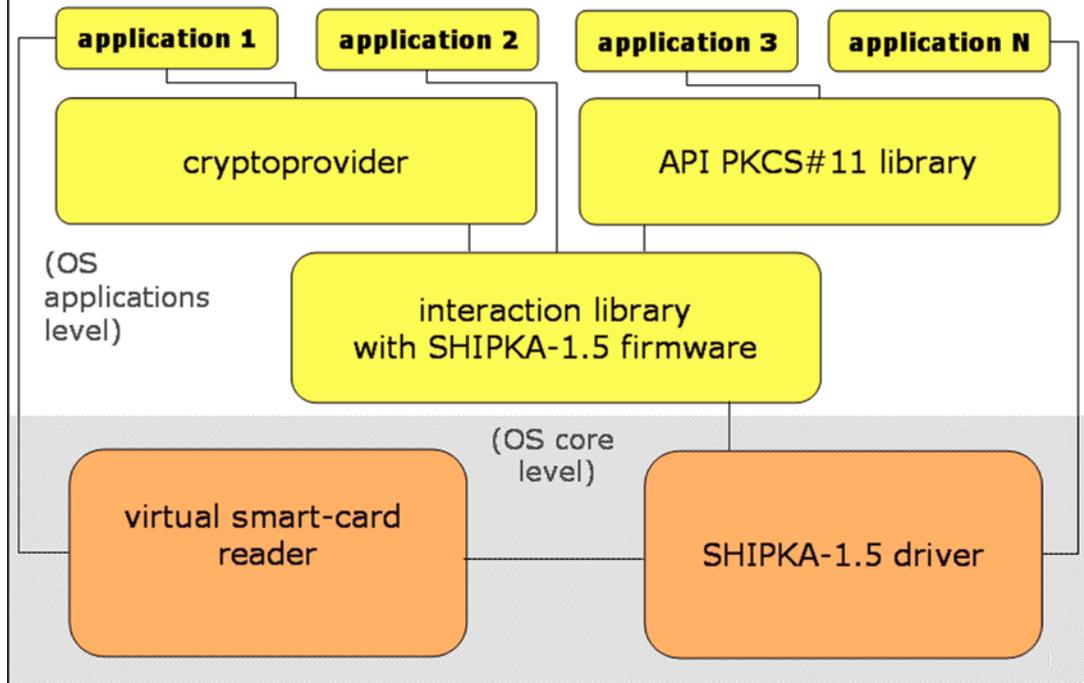
This also means that neither during a working session nor after switching SHIPKA off, the secret key information doesn't get into the computer's memory and cannot be intercepted or restored by an intruder.

SHIPKA-1.5: hardware

USB-controller

(Transport Level)

Protected MCU

core (ALU)

Firmware commands memory:
- cryptographic library
- functions of the file system (FS), similar to ISO 7816-4

SPI

Critical data memory

(Functional Level)

Hardware-based random number monitor

FS Data Flash data memory

SHIPKA-1.5: software

application 1 **application 2** **application 3** **application N**

cryptoprovider

API PKCS#11 library

(OS applications level)

interaction library with SHIPKA-1.5 firmware

(OS core level)

virtual smart-card reader

SHIPKA-1.5 driver

SHIPKA-1.5: software & hardware

| application 1 | application 2 | application 3 | application N |

cryptoprovider

API PKCS#11 library

(OS applications level)

interaction library with SHIPKA-1.5 firmware

(software)

(OS core level)

virtual smart-card reader

SHIPKA-1.5 driver

USB-controller

(Transport Level)

(hardware)

Protected MCU

core (ALU)

Firmware commands memory:
- cryptographic library
- FS Functions

SPI

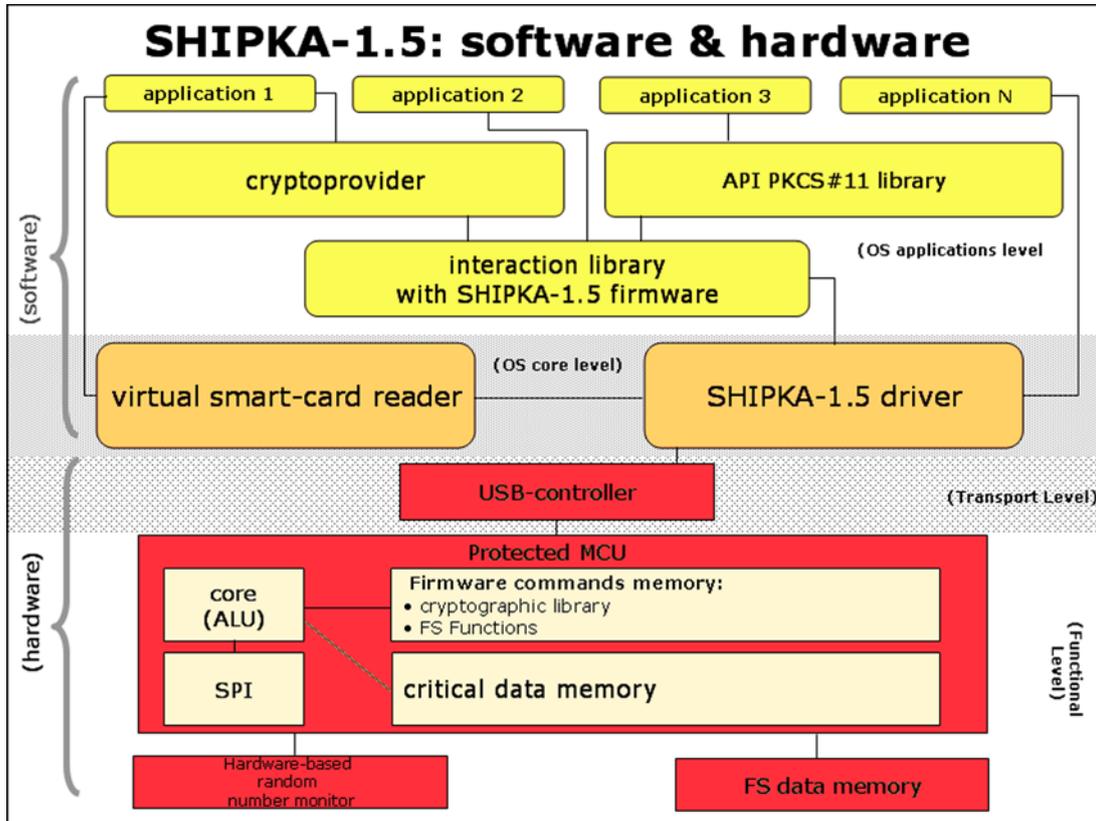**critical data memory**

(Functional Level)

Hardware-based random number monitor

FS data memory

You can use the encryption and Electronic Digital Signature possibilities at any computer, because all of the **keys are stored in SHIPKA**. This is absolutely natural – these are your secret keys, not the keys of your computer.

The file system support allows storing various information as files **in the data memory** of the Data Flash. This is not just the keys and certificates, but the user's personal data, his passwords for all kinds of web-services, the user software and all other required information.

However, this doesn't mean that anyone, who gets a hold of your SHIPKA, will automatically get a hold of all of the information that it contains – the access is protected by a **PIN-code** and in case the intruder exceeds the admissible number of incorrect tries, the device gets locked and all of the information gets erased.

The SHIPKA device is fully programmable, which allows to easily expand its functionality, updating the firmware without any additional equipment required – **through a WEB-service**. This is quite important, because the development of SHIPKA's abilities will go on and you will always be able to simply update your copy of the device instead of purchasing a new one each time.

Summarizing, we see the evident – with the help of PCIPT SHIPKA, you may solve an entire spectrum of the most urgent tasks of providing the security of the information interoperability.

At the present day, OKB SAPR is offering a range of ready-made solutions, using the PICPT SHIPKA.

In the first place, it's the **files encryption and their Electronic Digital Signature signing**. As it was said before, for this purpose you can select one of the Russian or foreign algorithms, hardwired in the device.

The second important possibility, offered by SHIPKA, in our opinion, is the **automatic filling of the web-forms** and storing all of the required data, including passwords.

Besides that, PICPT SHIPKA may be used for the **hardware identification and authentication of the user** on PC and notebooks, as well as in the terminal solutions like the "thin client".

For those of you, who don't want to use the cryptographic library, embedded into SHIPKA, but other cryptographic applications, we suggest using SHIPKA as a **protected storage for the encryption and signature keys and a hardware-based random number generator**.

PICPT SHIPKA may be used **as a "smart-card"** in the template solutions, using the smart-cards. These are the solutions like entering the Windows

domain, encryption and/or signing of the messages in the mail programs using various standards; obtaining the Verification Center certificates for the pairs "user name + his public key" – for using the PKI space.

PICPT SHIPKA may also be used for the **information technologies protection** with the help of authentication protection codes – for example, when constructing the protected electronic document management systems or other data processing systems.

Understanding the requirements of the participants of the information interoperability, together with our colleagues and partners, we keep working on the solutions with using the PICPT SHIPKA possibilities, which is why the presented list of solutions is not final.

It will be updated constantly and we will gladly inform you about it.

Moreover, we don't back-out of our rule and are ready to develop special SHIPKA versions with a set of features, **defined by the customer for his specific goals.**

Using the solutions with the smart-cards is very popular now and, offering to use SHIPKA as a smart-card, we cannot forget to mention **the advantages of this choice.**

First of all, the PICPT SHIPKA is a **USB-device** (Vendor ID OKB SAPR in the USB-association - 17e4); therefore, you don't need any card-readers to use it.

Card-readers are quite expensive devices, and if you're working at several computers – you will need a card-reader for each one of them or to carry a portable card-reader with you.

That means that using SHIPKA in such solutions is **both more convenient and cheaper**. This being said, SHIPKA is not in any way inferior to the smart-cards, moreover, it actually combines their possibilities with a whole variety of other possibilities that the smart-cards don't possess.

At the Cryptographic Information Protection Tools market, a range of USB-keys is presented as the high-functionality personal tools. In order to demonstrate the advantages of the PICPT SHIPKA, it's enough to compare its key figures by the most important characteristics (from the consumer point of view) with the key-figures of other devices, presented at the Russian market today.

To make a comparison, we have taken **SHIPKA-1.5** (the cheapest SHIPKA version, characterized by the least key figures) the eToken PRO device (as the most popular version) and eToken RIC (as the only

one of all of the foreign keys, which features the realization of the Russian encryption algorithms by GOST 28147-89), as well as the ruToken device (as an example of a domestic product).

Obviously, if we are talking about the tools of **CRYPTOGRAPHIC** protection of the information, the key figures for the consumer are going to be the figures that are related to cryptography, that is, a possibility of choosing among the hardwired cryptographic algorithms and the speed of the cryptographic operations.

Thus, **eToken PRO** has **6** hardwired algorithms and all of them are foreign: RSA, DES, TripleDES, SHA-1, MAC, iMAC. **eToken RIC** has **3** algorithms: foreign DES, TripleDES and Russian GOST 28147-89. **ruToken** has **1** algorithm – GOST 28147-89. **PICPT SHIPKA-1.5** has **14** hardwired cryptographic algorithms – **10** foreign ones and **4** Russian ones.

The encryption speed of SHIPKA-1.5 by GOST 28147-89 is **10 times higher**, than the speed of eToken RIC and **100-200 times higher**, than the speed of ruToken. These numbers don't seem to require a detailed comment.

There's also another significant parameter that should be added. All of the three devices use the Low-speed USB-controllers, while the PICPT SHIPKA has a Full-speed controller, that is why **the speed of the data exchange by the USB-interface** of the PICPT SHIPKA-1.5 outperforms all of the mentioned keys **by 25 times.**
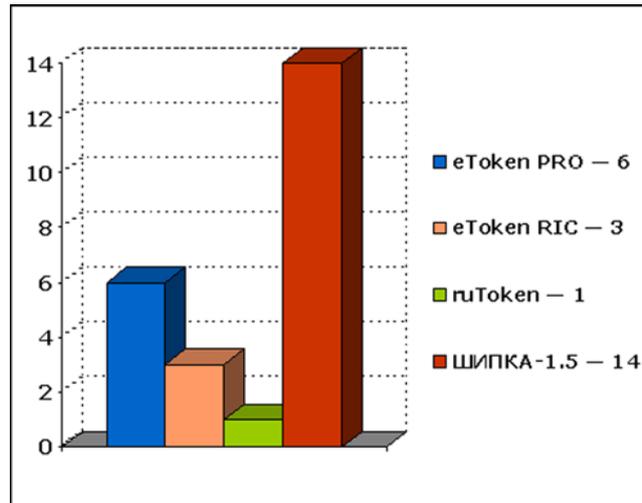
At the firmware level, in the PICPT SHIPKA, there have been realized the cryptographic library and the support of the file system, similar to ISO/IEC 7816-4; as well as the possibility of firmware updating **(note that no other devices, other than SHIPKA, have such an opportunity.)**

As it has been said before, in the PICPT SHIPKA, the following procedures have been realized at the software level: the transport procedures and the data formats coordination procedures. It's the driver of the device, the library of interaction with the firmware, the cryptoprovider, the API PKCS#11 library and the virtual smart-card reader's driver. The cryptoprovider of OKB SAPR for the PICPT SHIPKA **is signed by the Electronic Digital Signature of Microsoft**, which confirms its performance on OS Windows.

So, we have made the personal information environment both mobile and protected. In order to maintain protected information interoperability, you don't need to carry a computer around with you. A personal cryptographic information protection tool SHIPKA will do it for you.

IT'S A SIGNIFICANT EASE FOR YOUR LIFE!