COMPANY AKTIV

CREATING A SECURE CRYPTOGRAPHIC ENVIRONMENT AT THE STATE LEVEL FOR THE EXCHANGE OF ESSENTIAL INFORMATION

2021

About AKTIV company

Manufacturer and developer of software and hardware for cryptographic protection of information under the Rutoken and Guardant brands

A visionary company with its own technology ecosystem and extensive partner network worldwide

No. 1 in the strong authentication, e-signature and software protection market in the countries we operate in

We offer integrated solutions fully competitive in the global market

27 years in industry

500+ active partners

30+ million of Rutoken devices deployed

100+ cybersecurity experts on staff

What we offer for state structures

Ready-made platform solutions to build an independent national information security infrastructure in a consortium with the state authorities and local IT companies

Consulting in the field of cryptography and development of software and hardware solutions for information security

Preparation of the talent pipeline for the implementation of the national information security program

Representatives of the company

Konstantin Chernikov

Director-General

Timofey Matrenitsky

Head of International Business Development

«We see significant potential in developing cybersecurity infrastructure in the Middle East, have ready-made solutions and are focused on long-term mutually beneficial cooperation with our partners in the UAE, Turkey and other countries in the region.»

K. Chernikov

Secure cryptographic environment is a base for national information security

Information security starts with national standards that regulate the rules for creating, storing and sharing information

In the modern world, only a few countries have independent cryptographic solutions (USA, Russia, China and a few more), the rest are based on ready-made solutions, mainly originating from the United States. Most of them are not autonomous and not secure

User identification and authorization must take place in a secure environment, which is formed by a public-private partnership under the leadership of state and law enforcement agencies

Russian cryptographic solutions

- Russian solutions in the field of information security occupy the leading positions in the world. Only political factors prevent their spread
- Historically, the view of Russia was different from the view of the Old Europe and the United States — it is partnership and mutual development, not subordination to its own interests
- Currently Russian companies are developing complex cryptographic solutions for the benefit of government agencies in the CIS countries and some developing countries
- The approach of Russian specialists aims to create joint solutions in a consortium with local companies, establish joint ventures, and proceed to a joint development of technologies

Application scenarios

for the state segment

Organization of remote work of medical personnel, police and other services

Modern medicine requires the work of multifunctional medical teams to ensure the field work of medical personnel. Doctors from such teams have the necessary equipment to diagnosticate on the ground, as well as mobile devices to consult colleagues, organize treatment and hospitalization, order medicines via the Internet. Rutoken devices provide secure two-factor authentication of doctors in private accounts, which simplifies the preparation and signing of protocols right at the time when doctors are on call and examine the patients. Rutoken devices protect the access to confidential information, including personal data of patients.

Collecting tax reports

Using the Rutoken device an entrepreneur can benefit from electronic signature of documents for sending reports to the tax authorities. This allows to reduce the resources needed for processing tax reports, thereby increasing the speed of the tax service work and increasing the rate of tax collection at the state level.

Combating counterfeit goods

Rutoken devices are used for labeling medicines, alcohol, jewelry, as well as any consumer goods, which allows to control the volume of production and the turnover of these products. Labeling allows to make the market absolutely transparent, with the possibility to track the product at all stages - from production to retail sale. The ultimate goal of the introduction of labeling is the complete eradication of counterfeit and "grey" products on the market.

Remote electronic voting system

Rutoken devices provide citizens with access to the online voting platform and its functions needed for successful work within the framework of elections with the maximum level of security, transparency and verifiability. Remote electronic voting greatly simplifies the process of voting by citizens in the framework of election campaigns, by shareholders in the framework of shareholders' meetings, etc., including voters with disabilities, as well as those who are abroad.

Application scenarios

for the state segment

Electronic health system

The Unified medical information and analytical system was developed on the basis of Rutoken devices and integrated in the urban infrastructure. The system gives access to an "electronic registration office", which allows to make an appointment with a doctor remotely, reschedule an appointment without prior cancellation, find the polyclinic which is the nearest to your place of residence, and much more. More than that, there was developed a service, which allows to control the patient flows, issue electronic prescriptions and elaborate consolidated management records, it also contains an integrated outpatient medical record. In addition, the system contains information about the workload of medical institutions and the demand for doctors and allows to manage medical registers, solving medical and organizational tasks in relation to various categories of citizens with certain diseases.

Electronic passport system

The Unified identification and authentication system is functioning on the basis of Rutoken devices, this system is used for authorization in different state information systems. The main functional features of the system include: identification and authentication of users, management of identification data, authorization of authorized persons from executive authorities, collecting information about the user permissions in relation to information systems.

Safe sale of private property

Rutoken devices allow to conduct transactions with real estate, cars and other private property, carrying out a secure remote transfer of ownership from the seller to the buyer.

Secure electronic tenders and public procurement

Participation in tenders, auctions, procurements and quotations is impossible without a special ES for bidding. An electronic signature is needed to register on electronic trading platforms, submit documents and sign contracts in case of winning. Trading platforms generally allow the use of only an enhanced qualified electronic signature, which can be generated using the Rutoken token. Electronic documents signed with such a signature have the legal force of paper documents with signature and seal.

Ways of joint cooperation

Joint development of the cryptographic environment concept at the state level and elaboration of national standards. Consulting in this area

Creating co-production for key equipment (token / smartcard) for secure user authentication on the local territory

Creation of Cyber Security Infrastructure at the State level to implement the National cybersecurity strategy

Implementation of specialized secure solutions for government agencies, for example, solutions for Tax service, Health Care, Trade Control etc.

Solution for a Ministry as an example

- Unified user authentication system and electronic key management
- All significant employees have tokens or smart cards for authorization in the system
- The user actions history is registered, the information is protected from the majority of penetration types

Solution in Healthcare as an example

- Signing prescriptions from doctor's smartphone / tablet / PC
- Sign and encrypt records in patient's story
- Two-factor authentication in PC's and other devices with accents to patient personal data

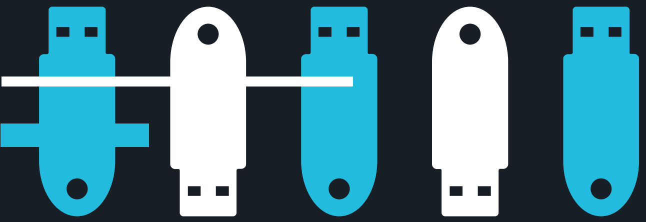
Creation of State Certification Center

One root state Certification Server with self signed certificate with mirror sites

State Certification Servers for particular state agencies (e.g. Tax Agency) that sign certificates for their clients

Private Certification Servers with accreditation that sign certificates for commercial clients

Two-Factor Authentication (2FA)



Passwords are not secure

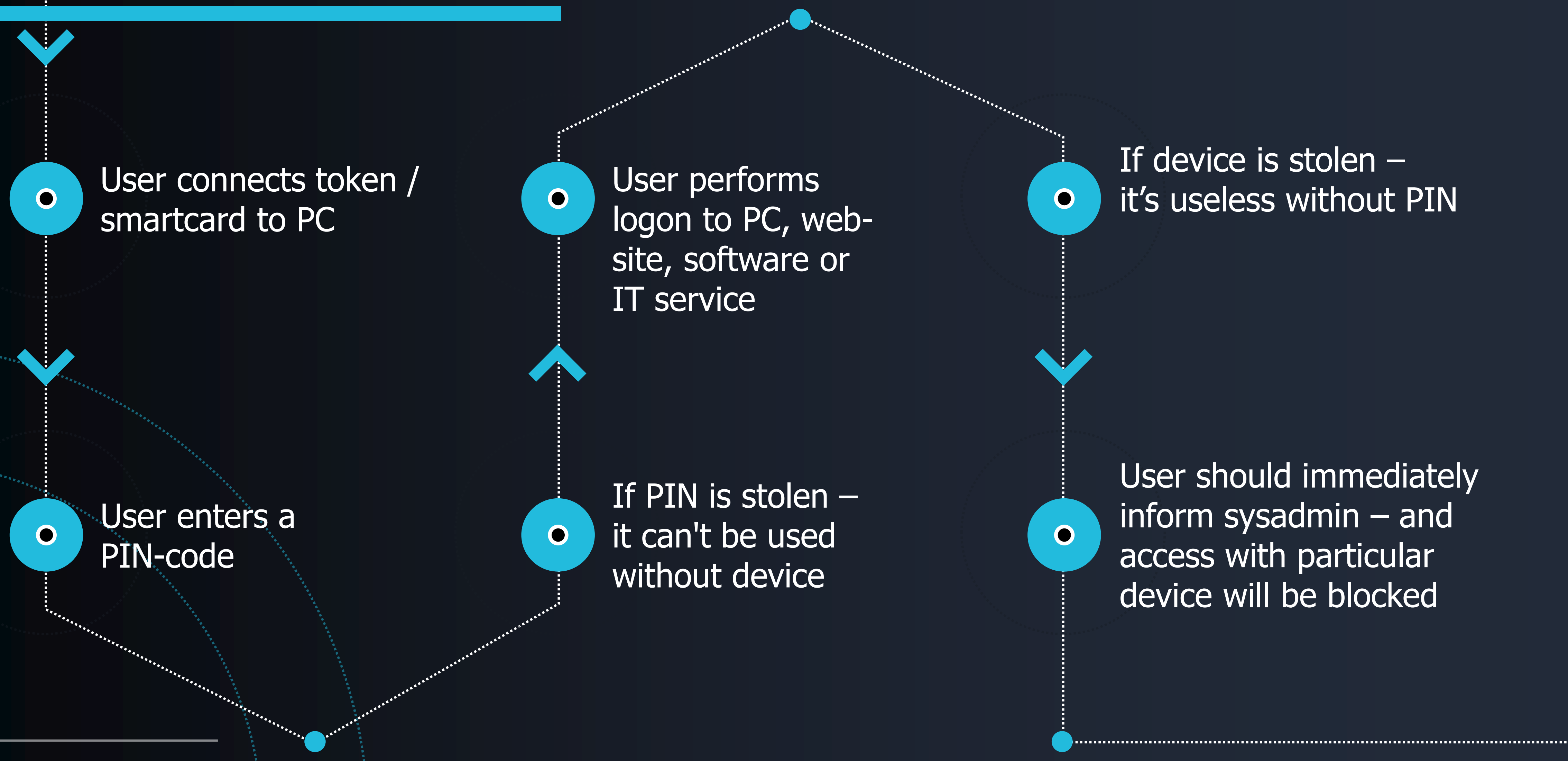
They can be stolen easily.
Strong password policy can’t help.

Two-factor authentication provides the real security

First factor – user owns a physical device (USB-token or smartcard)

Second factor – user knows the token / smartcard PIN-code

2FA Process



User connects token / smartcard to PC

User enters a PIN-code

User performs logon to PC, web-site, software or IT service

If PIN is stolen – it can't be used without device

If device is stolen – it’s useless without PIN

User should immediately inform sysadmin – and access with particular device will be blocked

We stay in touch

Timofey Matrenitsky

Head of International Business Development

+7 903 013 54 45 (WhatsApp, Telegram)

mta@guardant.com

www.facebook.com/matrenitskiy

www.aktiv-company.com

Thank you for attention!

2021

COMPANY AKTIV