Key components
to create a secure trusted IT infrastructure

– Protection of important information assets

– Secure remote access

– PKI for Linux

SECURE BY DESIGN

2024

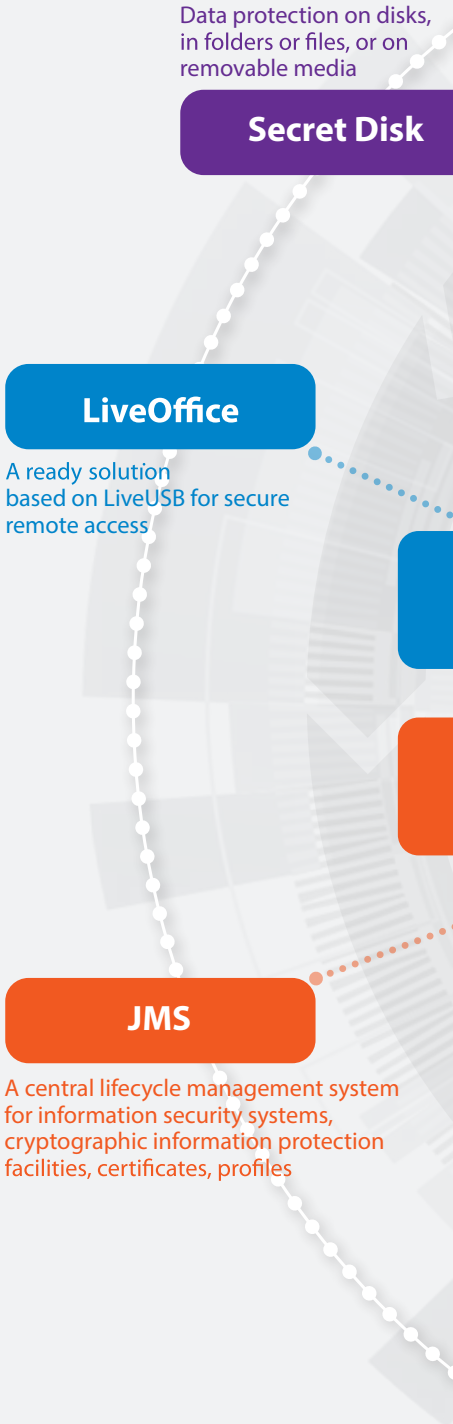
Products & Solutions

Solutions

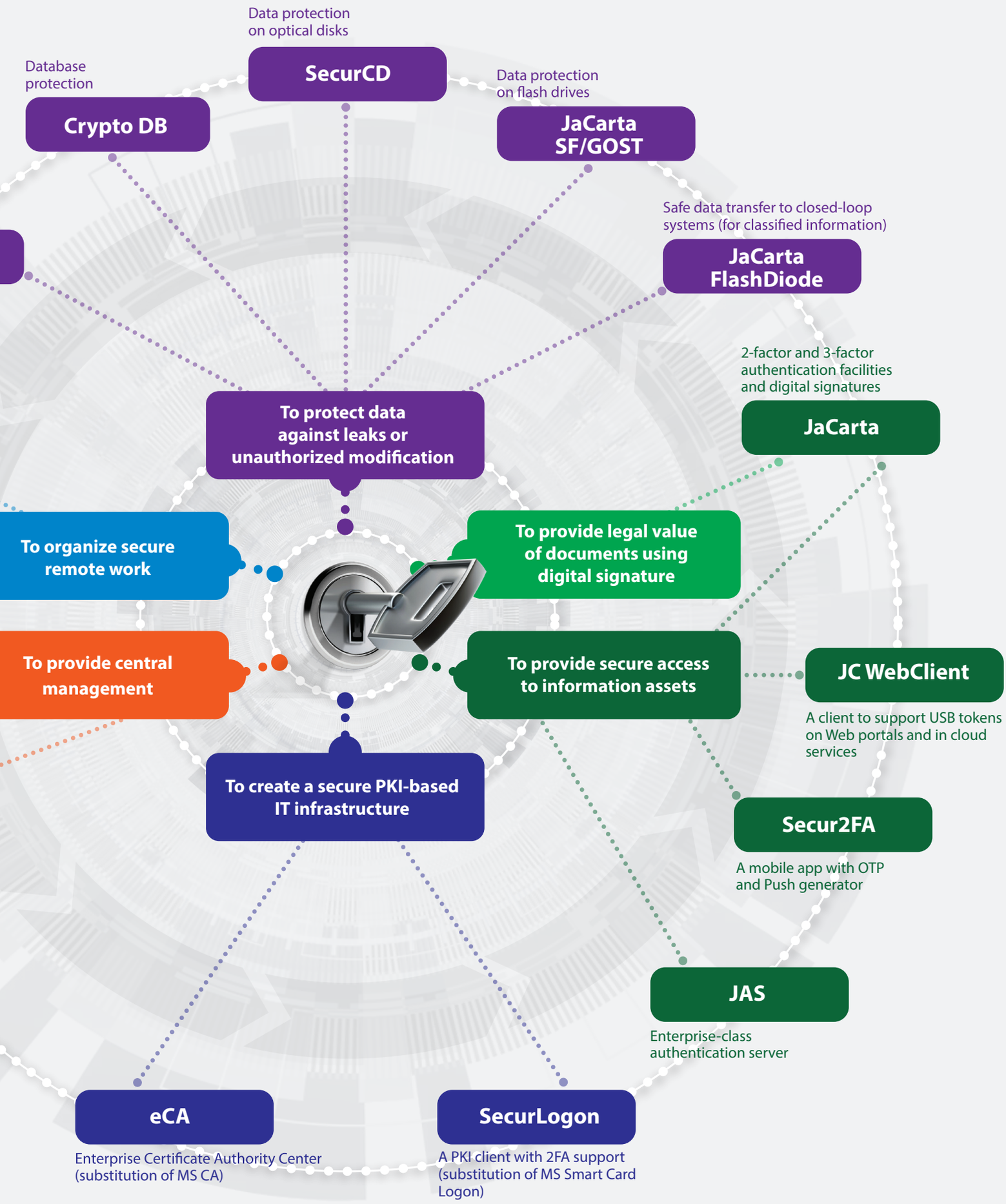
- To implement a PKI-based trusted secure IT infrastructure for any company
- To provide reliable identification and authentication of information system and online service users or devices (M2M, IoT)
- To organize secure remote work for employees and contractors
- To protect valuable information on servers, laptops of employees or removable media
- To provide central management of security facilities, certificates, profiles or policies

For:

- Government agencies, critical information infrastructure organizations, military industrial complexes
- Corporate users with a complex developed IT infrastructure
  - implementing Unix bound to continue using Windows
  - bringing their automated systems, geographical information systems, personal data management systems, automated control systems and critical information infrastructures compliant to information security requirements
- Enterpreneurs or individuals using public online services with digital signatures



All products are developed according to **Secure by design** principles – first comes the security followed by functionality.


Data protection on optical disks
SecurCD
Database protection
Crypto DB
Data protection on flash drives
JaCarta SF/GOST
Safe data transfer to closed-loop systems (for classified information)
JaCarta FlashDiode
2-factor and 3-factor authentication facilities and digital signatures
JaCarta
To protect data against leaks or unauthorized modification
To organize secure remote work
To provide legal value of documents using digital signature
To provide central management
To provide secure access to information assets
JC WebClient
A client to support USB tokens on Web portals and in cloud services
To create a secure PKI-based IT infrastructure
Secur2FA
A mobile app with OTP and Push generator
JAS
Enterprise-class authentication server
eCA
Enterprise Certificate Authority Center (substitution of MS CA)
SecurLogon
A PKI client with 2FA support (substitution of MS Smart Card Logon)

JaCarta

authentication solutions and digital signatures

- USB tokens
- Smart cards and readers
- Embedded security modules

› **two-factor** user authentication:
  – strong – PKI-based authentication
  – enhanced for IT infrastructures without PKI

› **three-factor** authentication using fingerprint biometrics.
  – Enhanced user identification is very important when accessing critical information resources of a company or while large financial transactions.
  – Biometrics ensures enhanced authentication.

› **digital signature** (including enhanced qualified digital signatures) in corporate and governmental systems of documents automation, on Web portals.
  – All cryptographic algorithms are implemented on a hardware level[1], private keys stay on a chip and cannot be stolen or cloned so, unlike software cryptographic information protection facilities, the keys are valid for 3 years instead of one.

› to apply tokens and smart cards in a corporate infrastructure as:
  – **a personal authentication and digital signature solution** to safely access the information system of a company, to work with electronic services and provide legal value of documents;
  – **an automated digital signature solution** in automated systems having longer life – over 10 mln signatures;
  – **an employee ID card** (badge) with the name, photo and position of an employee, proximity pass card (an RFID tag for an access control system) to enter company premises, user two-factor authentication or digital signature;

› to work on different devices and in various environments running:
  – Windows;
  – Linux;
  – Mac OS;
  – Android;
  – Aurora OS, etc

1. – except JaCarta LT model

JaCarta

account protection solutions for online services

JaCarta U2F

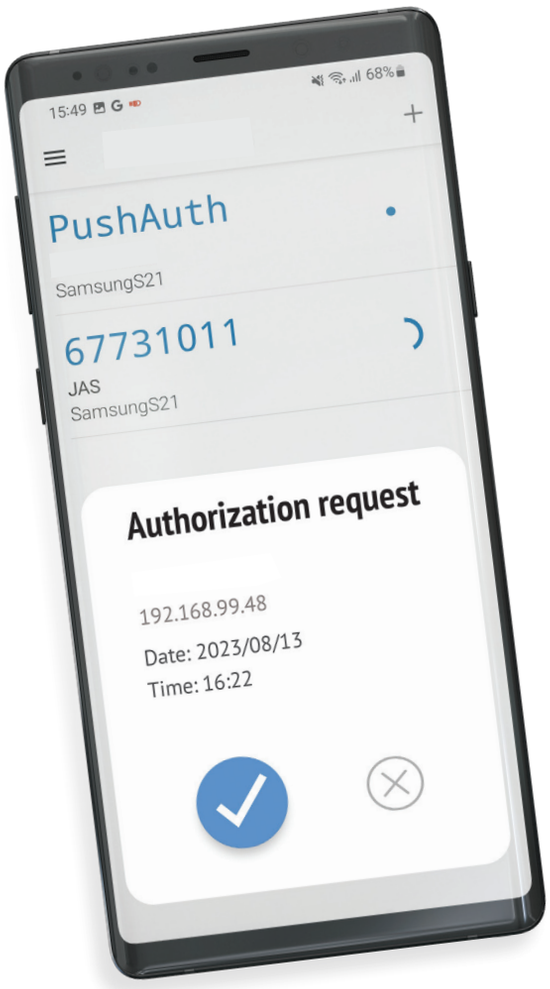
- supports FIDO U2F standard—a single token for all used electronic services — access to cloud or email services, video or file hosting, IT projects on GitHub, social media, etc.

JaCarta WebPass

- more convenient alternative to traditional OTP tokens when you need to manually enter a one-time generated password

authentication and OTP generation button

- to protect against fishing—to keep addresses of frequently used web resources and automatically follow them;
- to generate one-time passwords (OTP) and automatically fill it into corresponding forms;
- to generate, safely keep and automatically insert reusable comple passwords into the corresponding fields in screen forms;
- to provide enhanced two-factor authentication in infrastructures without PKI.



Smartphone Instead of Token

Secur2FA mobile app allows to use a smartphone instead of a hardware OTP token to provide enhanced authentication for computer, corporate network, different e-services.

It is more secure than SMS one-time passwords or software OTP generators, like Google Authenticator.

Central Management

Different tasks management in accounting, inventory, central management of JaCarta token and smart card lifecycle, certificate issue/revocation, accounting of cryptographic data protection, automatic report generation according to regulatory requirements, updating profile, automation of most routine operations using JaCarta Management Systems (JMS).

Enterprise CA

Certificate Authority Center on Linux (alternative to MS CA)

- to create and operate public key infrastructure (PKI);
- to manage digital certificate lifecycle;
- to join all IT infrastructure components into a single security domain, authenticate and provide secure interaction;
- to automatically maintain infrastructure objects and components using keys and digital certificates:
  - domain controllers, servers, web servers, email;
  - routers, firewalls, VDI, VPN, RDP gateways;
  - computers and other devices in domains;
  - M2M, IIoT devices;
  - users;

- to implement a PKI-based trusted secure IT infrastructure in complex heterogeneous, cloud and multi-tenant infrastructures;
- to provide scalability, failover and splitting of roles:
  - each functional role of a certification center (CA, RA, WebEnrol, CDP, DB, etc.) may be deployed on a separate server in a failover configuration..
- to work alongside active Microsoft CA;
- to import and use current Microsoft CA certificate templates or create new ones;
- to work with different directory services simultaneously (both Windows and Linux):
  - MS Active Directory, Samba DC, FreeIPA, ALD Pro;
- to integrate with different external systems using REST API:
  - IdM, IAM, IGA, SIEM, JMS, etc.;
- to provide strong two-factor authentication (in Linux, as well);
- to use different architectures of hardware platforms, national OSs,
- virtual environments.

SecurLogon

- full-featured PKI support, two- and three-factor strong authentication in Linux, Windows, macOS, and in mixed heterogeneous environments;
- working with Microsoft AD, FreeIPA, Samba DC, ALD Pro domains;
- enhanced user authentication using an automatically generated complex password up to 63 characters for infrastructures where PKI is not deployed yet.
  - The password is kept in the protected memory of JaCarta tokens, according to the current security policies, it may be automatically changed, for example, once a day or after each use.
  - After using a correct token PIN code, SecurLogon uses the password for domain and/or local authentication on standalone automated workstations.
- enhanced user authentication with one-time passwords (OTP) or a virtual token on a mobile device;
- applying logon policies based on user membership in a security group (token only / token or password / password only);
- authentication using any method on standalone AWPs or AWPs in peer-to-peer networks (a workgroup);
- extra service features allowing to unlock a token, change a user PIN-code, customize a welcome screen, etc., before logon to an OS;
- group deployment and remote setup from an administrator workstation;
- a full-featured alternative to Microsoft Smart Card Logon in the national Linux-based OSs;
- protection of remote connections (RDP, SSH).

Aladdin LiveOffice

secure remote access solution

Corporate PC alternative
with a set of installed apps and protection tools.

- to provide anything you need for working remotely from any untrusted computer, for example, home PC:
  - in geo-information systems, critical information infrastructures, automated control systems, medical information systems, etc., up to protection class 1;
  - in personal data management systems up to protection class 1 of personal data.
- to process personal data;
- to process commercial or business secrets:
  - in taxation, medicine, banking, notarial services, audit, defense, etc.;
- to protect against internal violators — a user cannot:
  - copy, print or forward any internal documents;
  - allow a third party use their account or compromise an account, password, connection settings;
  - upload a trojan or another malware to an information system.

- to save costs (5–7 times) while organizing remote work for employees or contractors;
- to automatically comply with all requirements and security policies;
- to be fully compliant with the requirements of safe remote work;
- to use Aladdin LiveOffice USB device as a remote workstation (a terminal) with a preset and preconfigured software working in a closed trusted hardware and software environment instead of a corporate PC;
- to provide central management using JaCarta Management System (JMS).

JaCarta Management System (JMS)

enterprise central management system

- to keep records and manage lifecycles of:
  - tokens, smart cards, cloud, software tokens, OTP/PUSH/SMS authenticators, U2F tokens;
  - removable media;
  - smart card readers;
  - secure remote work facilities;
  - information security systems, cryptographic information protection facilities, certificates, PKI objects, profiles;
- to automate most routine operations and security policy application (for example, PIN-code requirements);
- to quickly prepare typical profiles, configurations for different user groups, to enter new facilities into service, management of facilities used before implementing JMS;
- to access a convenient self-service portal (a web portal).

- to be integrated with external resource systems – sources of information about users or workstations, cloud signature service CryptoPro DSS, etc.;
- to bind user accounts from different resource systems;
- to maintain authentication and electronic signature certificates issued by different certification authorities;
- to track and audit user or administrator activities that may be exported to a Syslog server to be integrated with SIEM;
- to automatically send notifications;
- to update device firmware, embedded OS and app images remotely and safely;
- to add necessary features due to developing and connecting extra modules and connectors;
- to use Linux or Windows version.

It includes:

- a high-performance Enterprise-class authentication server – JAS (optional).

JaCarta Authentication Server (JAS)

high-performance Enterprise-class authentication server

- to provide secure access of external and internal users to information systems and services:
  - remote access gateways CryptoPro NGate, UserGate, Microsoft, Cisco, Citrix, Palo Alto, Check Point, VMware, Fortinet, etc.;
  - gateways to Microsoft RDG desktops;
  - CRM, ERP, MS SharePoint, MS Outlook Web App, email;
  - web apps, cloud services;
  - remote banking services, electronic document flow and other systems;
- to provide enhanced and strong authentication:
  - in infrastructures without PKI;
  - in OSs based on Linux or Windows;
  - in services and apps using U2F-compatible tokens, OTP, SMS, PUSH notifications;
- to integrate with application software using standard protocols: RADIUS, REST, WCF, ADFS, HTTP, SMPP;
- to provide high failover (Failover Cluster) and performance over 5,000 authentications per second.

- to use different methods, means, protocols and facilities of user authentication:
  - almost any existing or new hardware USB tokens, OTP tokens compliant with RFC4226, RFC 6238, FIDO U2F;
  - mobile apps, like Yandex.Key, Google Authenticator, Secur2FA, providing secure initialization vector transfer and eliminating the risk of QR-code reuse, as well as implementing PUSH notifications;
- to track and audit user or administrator activities that may be exported to a Syslog server to be integrated with SIEM;
- to provide accounting and central management of facility lifecycle (integrated with JaCarta management system).

Secret Disk
data protection on disks

- to prevent leaks and unauthorized access to valuable information when computers, servers or disks are lost, stolen, withdrawn, repaired or disposed improperly;
- to encrypt data transparently:
  - on laptops, PCs, tablets[1] of employees;
  - on file servers and application servers (including databases);
  - on removable media;
- to hide valuable information on a protected computer, server or media;
- to completely and assuredly delete data;
- to prevent access to protected partitions on servers (databases, corporate email, etc.) in emergency situations after an alert;
- to securely transfer sensitive information over unprotected communication channels;
- to log any successful access to the protected information;
- to protect against actions of privileged users (system administrators);
- to provide central management and integration with JMS management system (for the Enterprise version).

- to encrypt:
  - a system partition[2] that contains information about a user account, logins and passwords for different information resources, licensing information, OS temporary files, swap files, log flies of apps, memory dumps, a system image stored on a disk when the device enters a sleep mode;
  - partitions on hard drives, logical disks, disk arrays (SAN, RAID);
  - virtual disks;
  - removable disks (USB or Flash-drives, etc.);
  - files and folders;
- to use two-factor authentication to access protected information (before OS boot as well);
- to provide access to encrypted files to other users;
- to protect data in backups created using third-party apps.

Secret Disk Versions

- **personal**
  (a common license for Linux and Windows)
- **server**
- **corporate**
  (Enterprise version) with central management features

1. – For Windows and Linux.
2. – For Windows only.

Crypto DB
database protection

- to protect main information assets of a company (ERP, CRM, information security systems, personal data management systems, etc.):
  - against leaks or stealing;
  - against unauthorized modification or spoofing of sensitive information;
  - against unauthorized access of database management system (DBMS) administrators (insiders) to critical data;
- to anonymize personal data;
- to transparently encrypt selective critical data in a DBMS;
- to provide two-factor user authentication when accessing data in a DBMS;
- to centrally manage encryption keys eliminating unauthorized actions of DB administrators;
- to implement regulatory authority requirements:
  - on providing privacy and integrity of information in a DBMS;
  - on personal data protection, PCI DSS (for systems using bank cards), information systems of organizations using critical information infrastructures;
  - access division models—discrete and mandatory.

For Oracle, MS SQL, Tibero, PostgreSQL, Postgres Pro, Jatoba

- to substitute integrated to DBMS foreign protection tools and continue using necessary DBMS and apps;
- to protect critical data in DBMS:
  - in client-server information systems;
  - in multi-tier apps of information systems;
  - in information systems with the terminal access;
  - in virtual and cloud infrastructures (IaaS, SaaS);
- to track and audit user or administrator activities that may be exported to a Syslog server to be integrated with SIEM;
- to create protected information systems using certified cryptographic information protection facilities;
- to get non-adjustable legally relevant evidential base to investigate information security incidents.

JaCarta SF/GOST

Information transfer control from computer storage removable media

- to securely store and transfer encrypted data;
- to provide data access only for authorized users and only from trusted computers;
- to protect valuable information against unauthorized access or copying, including:
  - flash-drive users (for example, when trying to copy data to a personal computer);
  - system administrators (for example, when trying to access critical data);
- to hide valuable information on a service flash-drive;
- to provide dual functionality:
  - as an identification or authentication solution;
  - as digital signature solution (enhanced qualified) with a non-retrievable private key in document automation systems

- to process and protect business, restricted information, classified information with "top-secret" sensitivity level;
- to implement information transfer from or to removable media;
- to configure a security policy:
  - neither administrators (when connecting locally or over the network), nor system processes (backup, anti-malware, etc.) can access data;
  - set up different levels of administrative permissions for a Chief Administrator and an Administrator doing operative tasks according to the configured policies or templates;
- to track and audit user or administrator activities that may be exported to a Syslog server integrated with SIEM;
- to meet legislation and regulation authority requirements to removable media

SecurCD

data protection on optical disks

- to provide secure and targeted transfer of encrypted sensitive information on optical disks CD/DVD/BR;
- to block integrated or special programs able to read/write data on optical disks, like Nero, UltraISO, etc., to prevent writing or transfer data in the clear (unencrypted) form;
- to make data readable by the recipient only using a private key;
- to protect data against external and internal violations.

- to process and protect restricted information, classified with "top-secret" sensitivity level;
- to track and audit user or administrator activities that may be exported to a Syslog server to be integrated with SIEM;
- to generate pairs of keys;
- to exchange public keys with contractors;
- to keep private keys in a protected JaCarta SF/GOST flash-drive and/or in a password protected file container;
- to work with a protected JaCarta SF/GOST flash-drive both with a plugin extending its functionality or without it.

JaCarta FlashDiode

one-way flash-drive to safely transfer information to closed-loop systems

- to safely transfer data from an open-loop information system to the closed-loop:
  - **restricted information** (for example, geographical information systems, medical information systems, critical information infrastructures, automated control systems, personal data management systems);
  - **classified information** with "top-secret" sensitivity level;
- to prevent hiding of unauthorized copying or transfer of information (its leak) from a closed-loop system (implemented in the architecture on a hardware level);
- to record data to a flash-drive on authorized computers by authenticated users only;
- to audit user or administrator activities.

- to stop using write-once optical disks (CD-R) and replace it with reusable flash-drives;
- to reduce the cost of automated system ownership:
  - disposal of media after using them in a closed-loop is not needed;
  - optical disk drives and corresponding control and protection tools are not needed;
  - no need for one-way USB gateways;
  - information transfer to a closed-loop system becomes easier (no need to re-qualify automated system);
  - employees and administrators save time
- to work in virtual environments (in an open-loop system);
- to safely update signature databases for anti-malware, system, application or integrated software (firmware of different devices), databases, etc.

- Key components to implement a trusted secure IT infrastructure for any company and protect its important information assets.
- Authentication tools and digital signature thus providing information security and data protection.
- Secure-by-design products and solutions for information security systems and information protection facilities including dealing with classied information.
- Most products may be used for working with information up to "top-secret" sensitivity level.

Providing customers of all sizes with products and solutions in:

- Information security
- PKI for Linux
- Multi-factor authentication, secure access to information assets
- Secure remote work for employees and contractors when they are not using trusted devices
- Authentication and digital signature for USB tokens, smart cards, IIoT devices, security modules (Secure Element), Web portals and electronic services
- Data protection (on disks or removable storages, in databases)
- Migration from MS CA (CS) to Linux based corporate certication center
- Transparent encryption on disks, flash drives, file servers or application servers
- Database protection
- Biometric identication and fingerprint authentication (Match On Card/Match On Device)
- Development of embedded Secure OS and cryptography for microcontrollers
- Trusted boot, sterilization of imported ARM processors with TrustZone, TEE and cryptography implementation