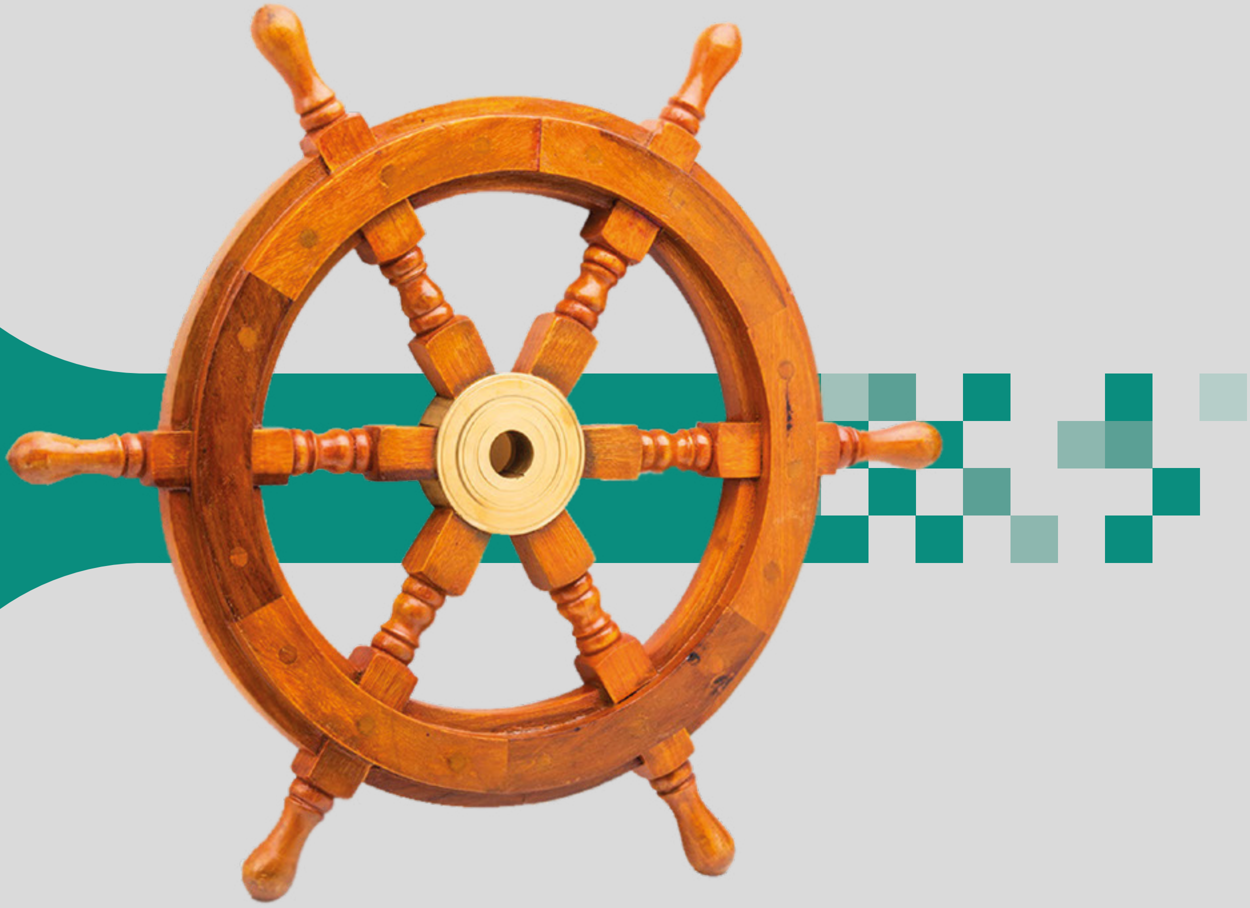
Enterprise Smart Card and Token Management System



JMS

JaCarta Management System

- Supports USB tokens and smart cards from various manufacturers
- Compliance with regulations of Russian cryptographic means usage
- Advanced audit of employee and administrator actions
- Low cost of implementation and support
- National regulator certificate

The Challenge of Enterprise Token Support

Any organization that uses tokens for employee authentication is faced with significant costs for their support, including token accounting, management, cross branch distribution, regulation compliance, and so on.

Token Accounting

How to associate the token with a user, department, or branch?

How to manage the purpose of a token (authentication, electronic signature, access control, etc.)?

How to manage the private keys and certificates on tokens? How to control certificate validity on a bulk of tokens?

Management

How to understand access to which system has the user by the token? How to enable or deny such access instantly?

How to examine which enterprise security policies are working?

How to find out access rights of the user groups? Are their rights sufficient?

How to issue certificates for large user groups quickly? What should you do if such groups are located in different branches?

How to keep the users' data and certificates actual while their circumstances change (such as changing the last name because of marriage)?

Authority Regulations Compliance

National regulations can be managed with several authorities (such as federal security services, custom or financial regulators, etc.).

For example, some national regulators require the per-instance accounting of licenses for program cryptographic means and the per-instance accounting of tokens as cryptographic means.

If a company uses hundreds or thousands of tokens, it takes a lot of time and efforts of information security department for their supporting, thus automation of accounting and management of tokens is necessary for organizations that:

- uses over 100 USB tokens and smart cards;
- needs to enforce compliance with information security policies or regulatory requirements;
- distributes authentication means across multiple branches.

Medium and large enterprises and corporations

Banks and other financial organizations

Public institutions, ministries, and departments

Purpose of JaCarta Management System

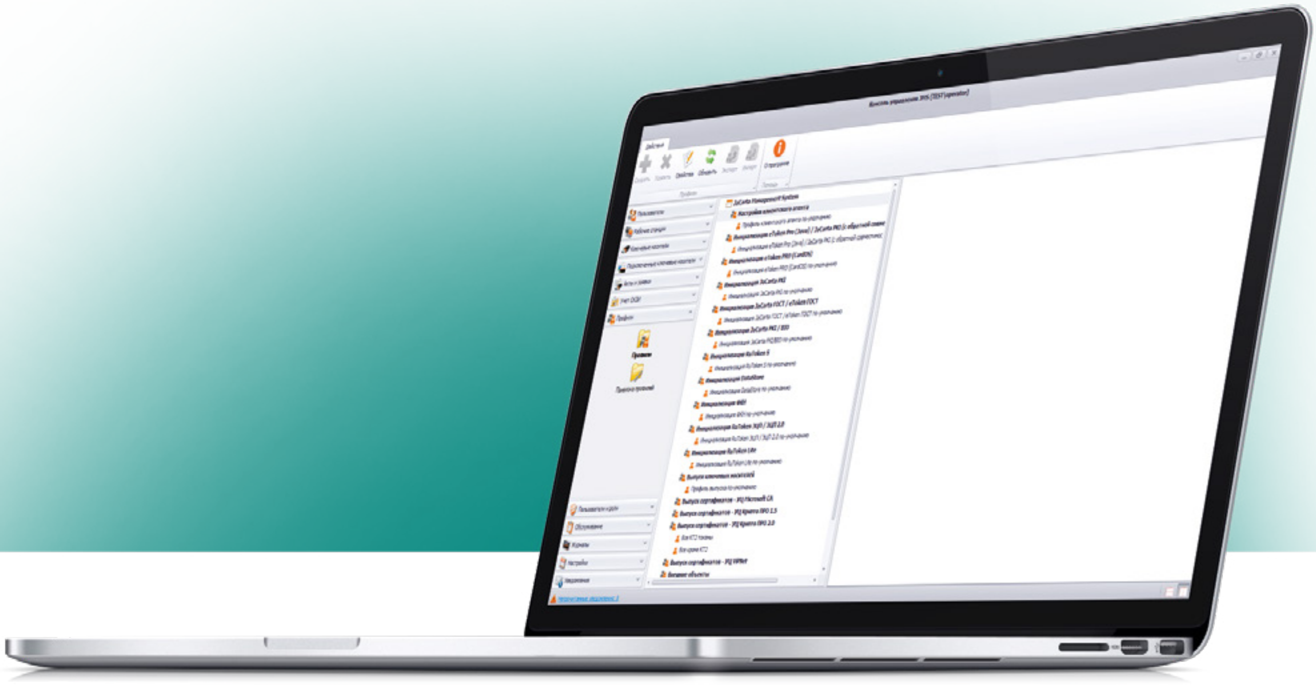
JMS is a corporate accounting and lifecycle management system for USB tokens and smart cards of various manufacturers (JaCarta, SafeNet eToken, etc.). With it, you can automate typical operations when working with USB tokens and smart cards, provide flexible configuration of policies for their use, as well as centrally control access to corporate systems.

The built-in reporting and printing tools in JMS allow you to track the status of devices and automate the provisioning of documents related to their life cycle.

The automatic synchronization of USB tokens of USB tokens and smart cards with the JMS database and widespread certificate authorities makes it possible to instantly bring the contents of the entire fleet of USB tokens and smart cards to the actual state.

"... Organizations with roughly 200 or more X.509 certificates in use that are using manual processes typically need one full-time equivalent (FTE) per year to discover and manage certificates within their organizations"

© Gartner, 2011 (G00226426)



Scope

Automated Tokens Accounting

JMS allows you to automate the accounting of all tokens. System stores the information about owner, number, model, operation time, stored objects and workstations which tokens were connected.

Token Lifecycle Management

JMS allows you to manage the entire life cycle of tokens from issuing to revocation, along with all the objects associated with them such as digital certificates, keys, etc.

Security Policies Management

Using JMS you can centrally manage security policies for tokens, changing applied policies almost instantly.

Ability to Work without Hardware Tokens

JMS allows you to issue certificates not into a token, but directly into the PC registry. Thus the user can now work without a token. Besides you can automatically collect information from user or computer certificate storage or from the file system on PCs which has JMS client installed on. All found certificates are taken into account in the system and their validity can be kept up to date by promptly updating expiring certificates following the administrator settings. The administrator can also remotely delete unwanted certificates on user PCs.

Document Creating and Printing

JMS can create and print applications for issuing, replacing and revoking tokens or digital certificates, making it as easy as possible to create documents related to the token life cycle.

Auditing User and Administrator Actions

JMS keeps a log of user and administrator actions with convenient search and sorting mechanisms to help diagnose problems and resolve conflict situations.

Synchronization with External Systems

JMS can automatically track changes in external systems (such as Microsoft Active Directory or certificate authorities), including change user attributes (for example, when changing the last name), reissue certificates and update them on tokens.

Support for Branch Network

JMS allows you to track the movement of tokens across branches and distribute rights to administer JMS servers between IT specialists at headquarter and branches. It is possible to issue certificates to a group of users distributed across different branches.

User Self Service

JMS allows an employee to independently perform token operations (issue, synchronization, block, unlock, replace) without contacting IT or information security departments.

Token Data Backup

JMS preserves copies of objects issued on the tokens. It ensures the information safety and restoring tokens with preserved certificates.

Reporting

JMS provides the reporting subsystem to create the token and workstations usage reports and the user activity reports. You can build reports by a separate organization unit and throughout the branch network.

JMS Management Console

Convenience

The JMS Management Console provides a user-friendly and intuitive graphical interface for administering users, tokens, certificates, cryptographic means, security policies, and maintenance plans. All functions for managing and accounting tokens are concentrated in one place, which eliminates the need to work with several separate applications.

For greater convenience, JMS Management Console can be switched to simple mode. It hides all objects and controls for which the operator does not have rights. This mode can be used for the comfortable work of Pass Office officers and local administrators who do not need all the JMS features.

Security

The JMS management console is a full-fledged Windows application. As opposed to web-based clients it guarantees fast and smooth operation, as well as eliminates such weaknesses as incompatibility issues with new browser versions and reduced security due to the use of ActiveX components or plug-ins for working with tokens.

JMS realizes role-based access control. So permissions to operations correspond to the specific role of console users. Data transfer between the JMS Server and the JMS Management Console is encrypted using the HTTPS protocol (SSL and TLS, including TLS version 1.2).

JMS Benefits

Improving Organization Efficiency

The implementation of JMS improves the efficiency of the information security department and the entire organization. This is achieved by automating work with tokens, significant reduction in the number of human errors, as well as reduced downtime for employees caused by breakage of tokens or expiration of digital certificates.

Unique Features

JMS has some unique features that allow you to significantly simplify work with tokens, reduce the number of errors and improve the efficiency of the IT department and employees.

- automatic accounting of cryptographic means under the national regulations;
- automatic token accounting;
- automatic certificates update upon change of personal data of users;
- support for multi-functional tokens;
- bulk registering of JaCarta tokens;
- issuing user certificates into the PC registry (not into tokens) and managing them;
- accounting the certificates in the user and computer storages on the PCs;
- "taking under control" legacy tokens and objects on them;
- preservation of replaced certificates;
- accounting for the movement of tokens between departments of the organization;
- managing the keys of external users (outside Active Directory);
- supporting the distributed architecture with standalone JMS nodes;
- distribution of the administrative access rights between branches;
- creation of customized requests to all supported certificate authorities;
- easy migration from SAM and TMS, including parallel operation of both systems (JMS and SAM/TMS) with the preservation of all data and settings.

National Regulations Compliance

JMS's ability to account both hardware and software cryptographic means ensures compliance with national regulations. JMS is also certified by the national regulator and can be used to protect information in public institutions with high requirements for information security.

Rapid Implementation

Due to an automating of installation and configuration process, as well as a number of unique features, such as bulk registration and "taking under control" of previously released tokens, you can deploy JMS in a short time. According to the experience of the Pension Fund of Russia after testing and setting up the JMS in the pilot zone, the process of implementing the system in each of the branches of the fund took on average just 3 days.

Scalability and Performance

JMS is designed as a high-performance and scalable system that allows you to account and manage more than 1 million tokens (and their internal objects) without noticeable performance degradation. JMS can work as a cluster in virtual environment or as standalone nodes in organizations with a geographically distributed structure which are lacking for channel capacity.

Simple User and Admin Interface

JMS provides a modern and intuitive interface for administrators and security officers. There is the JMS Management Console for such a type of user. The console allows you to manage all tokens, users, workstations and security policies, as well as build reports and maintain the system. In turn the JMS Client is addressed for end users. It allows you to synchronize tokens and use self-service functions. There is also the web based user account manager that has a friendly interface.

Support for Legacy Systems Based on PKI

JMS allows you to "take under control" the tokens that were used in the organization prior to JMS implementation, as well as preserving certificates and keys on tokens that are revoked. The system also supports all widespread certificate authority software. This allows you to ensure continuity with the legacy infrastructure and to avoid problems caused by the transition to a new token management system.

Native JMS Directory Service

If your organization does not have Active Directory or another directory service, JMS allows you to create your own directory of users with the necessary attributes and hierarchy of organization units (OU), which is customizable through the JMS Management Console. User profiles can be tied to different OU of the hierarchy, allowing you to quickly assign and modify desired security policies.

Low TCO

JMS provides transparent licensing schema. The basic JMS package already includes all the necessary functions for the full automation of accounting and management of tokens. Additional features are licensed separately. It allows you to optimize costs and plan a gradual development of the system. After the JMS is implemented, only technical support is paid. It allows you to receive Aladdin's support and all system updates.

Single Provider of Tokens and Management System

"Aladdin R.D." is the only Russian manufacturer that produces both the hardware means for authentication and electronic signature (JaCarta tokens) and the management system (JMS) for this means. If customers buy both, they get the following:

- the most simplified processes of logistics, implementation, and provision of technical support;
- reducing the cost of finding disparate suppliers, as well as testing and supporting unrelated solutions and products;
- reducing the total cost of supporting the means of authentication and electronic signature;
- guaranteed compatibility of products and the reliability of their joint operation;
- fast release of updates and support for all new models of JaCarta tokens;
- the ability to influence the further development of JMS and JaCarta tokens, offering new features;
- full support of widespread tokens and smart cards of other manufacturers.

Flexible Customization and Modification

The open API is provided, allowing integrate JMS with other information systems. For example, you can provide management of JMS users from another system, including import users and workstations to JMS, etc.

Licensing and Support

Licensing

- JMS is licensed only by the number of users whose tokens are controlled by the system.
- Within one version, the license validity period is not limited.
- You can purchase additional licenses by the piece.

Implementation

- A full-featured version for 1 month is available to explore JMS.
- Automated installing and configuring.
- The implementation and maintenance of JMS can be carried out by authorized partners of "Aladdin R.D.", as well as representatives of the manufacturer.

Technical Support

- When buying a JMS, 12 months of basic technical support is provided.
- Basic technical support includes the following:
  - getting all product updates within the major version (3.x);
  - getting advice on installing and using the system;
  - access to the JMS, JaCarta, and eToken Knowledge Base.
- Support packages for 12, 24, and 36 months are available.
- Extended technical support package including an individualized set of additional services is available.

Additional Options

- Support for biometric identification technology.
- Support for Entrust, Check Point, Microsoft, CryptoPro 1.5 / 2.0, ViPNet 4.6, and Notary-PRO 2.7 certificate authorities.
- Importing user data from CryptoPro 1.5 or 2.0 certificate authorities.
- Accounting of cryptographic means.
- Support for third-party tokens.

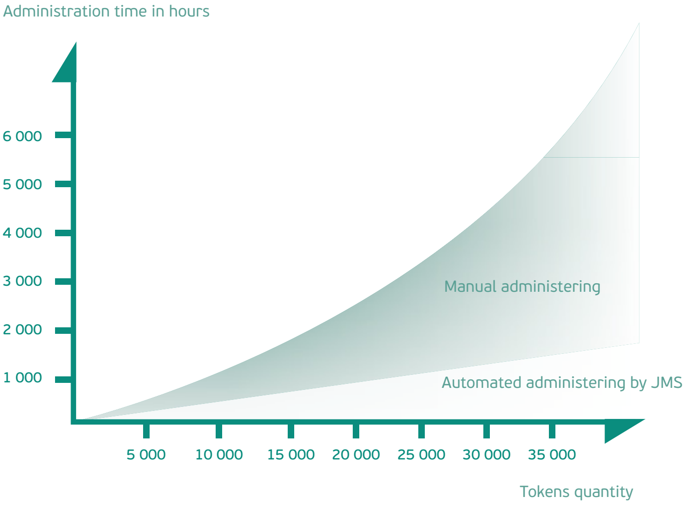
Economic Effect of JMS Implementation

JMS improves the efficiency of the IT and information security departments, reducing the time and operational costs of implementing and maintaining authentication and electronic signature means.

The savings in labor costs of a security administrator can be estimated by comparing the execution time of the most frequent operations with tokens in manual mode versus using JMS (see the table below).

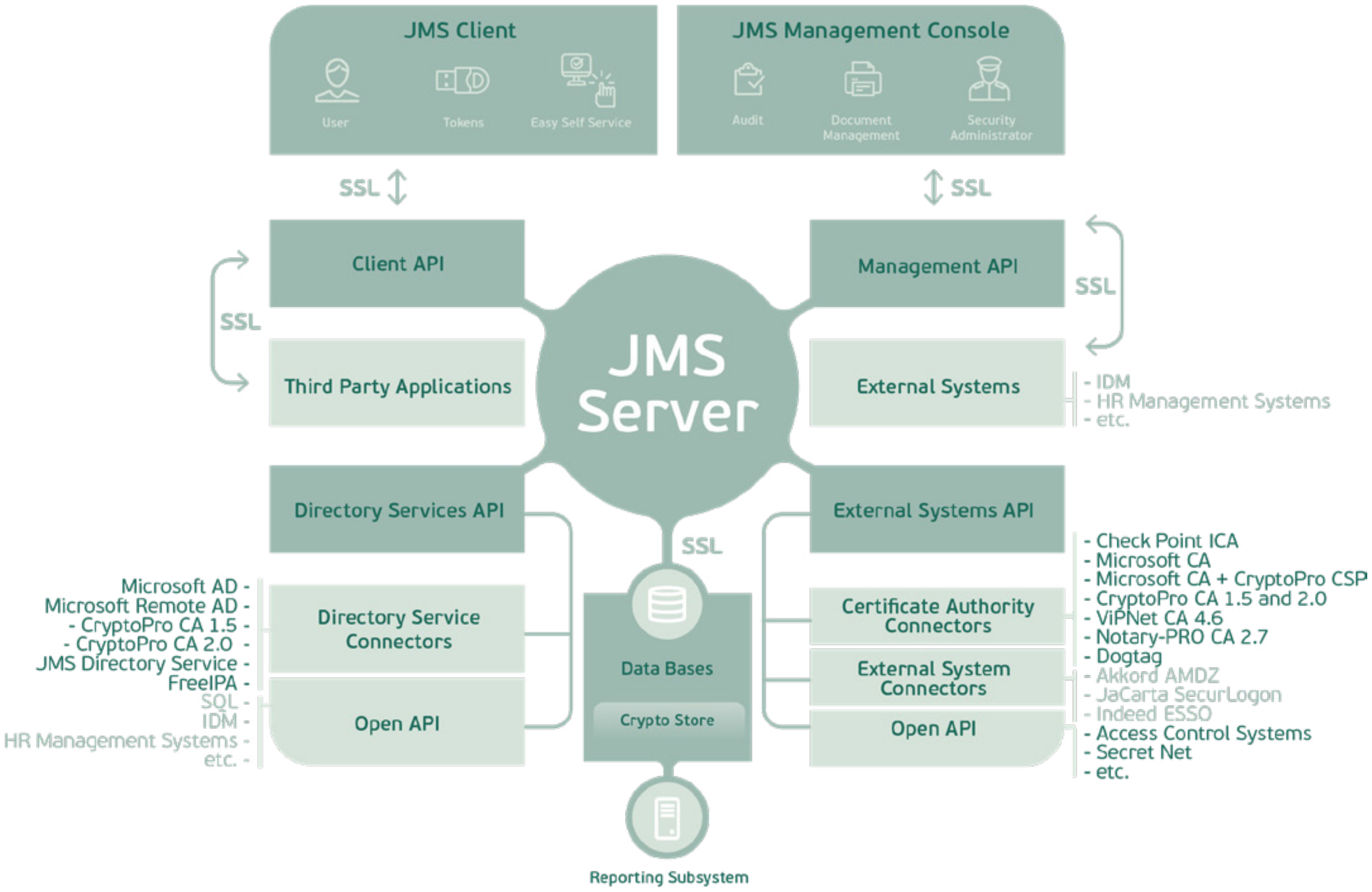
Operation	100 Tokens in Use			1000 Tokens in Use		
	Manually	Using JMS	Time Savings	Manually	Using JMS	Time Savings
Issuing a token and 2 certificates (authentication and electronic signature) to an employee	2 min	1 min	by 2 times	2 min	1 min	by 2 times
Issuing a token and 2 certificates (authentication + electronic signature) to each company employee	100 × 2 min = 3 hrs 20 min	5 min*	by 40 times	1 000 × 2 min = 33 ч. 20 min	5 min*	by 400 times
Revoking a token with 2 certificates (authentication + electronic signature) for an employee	2 min	30 сек.	by 4 times	2 min	30 sec	by 4 times
Revoking a token with 2 certificates (authentication + electronic signature) for each company employee	100 × 2 min = 3 hrs 20 min	5 min*	by 40 times	1 000 × 2 min = 33 hrs 20 min	5 min*	by 400 times
Issuing additional certificate to each company employee	100 × 1 min = 1 hr 40 min	5 min*	by 20 times	1 000 × 1 min= 16 hrs 40 min	5 min*	by 200 times
Reissuing certificates to all company employees upon expiry	100 × 2 min = 3 hrs 20 min	2 min*	by 100 times	1 000 × 2 min = 33 hrs 20 min	2 min*	by 1000 times
Remote unlock token PIN	2 min	30 sec	by 4 times	2 min	30 sec	by 4 times
Average Effect of JMS Implementation	**10 Times Lower**			**15 Times Lower**		

* In the case of mass servicing of users, the JMS administrator spends time only for enrollment profiles configuring and binding of their to the users. Further manual work is not required, which saves administrator time and reduces the possibility of errors.



For a method of calculating the economic effect of the JMS implementation, contact Aladdin's representatives or its partners.

Architecture



- **JMS Server** is the core, which provides centralized management of user accounts, tokens, policies, etc. It can be installed as a standalone node or as part of a cluster. JMS server part can be deployed in a virtual environment.

- **JMS database** is the centralized storage of information about JMS user accounts, tokens and their objects, policies, JMS settings, etc. Sensitive information is stored in the crypto storage.

- **Crypto storage** is a virtual object (database area) where critical data (private keys, PIN codes, etc.) are stored. The crypto storage is created during initial JMS configuring.

- **JMS Management Console** is an administrative console that allows you to register users, perform operations on user tokens, set up enrollment profiles, create and edit global JMS groups, and execute maintenance plans. The console allows you to restrict the authority of roles within the scope of specified organizational units and operations.

- **JMS Client** is a client application on the user side that performs the function of synchronizing the contents of the token with the data on the JMS server, and also allows the user to perform a series of token operations within the self-service (enrollment, unlocking, replacing).

- **JMS Server API** is an open API to develop connectors for certificate authorities and directory services, customer's proprietary software, as well as for integration with other enterprise information systems.

JMS Client

- Full-fledged Windows application (as opposed to competing solutions using a web interface) provides the following advantages:
  - fast and uninterrupted work is ensured due to operation in native Windows environment;
  - it's free of unavoidable reduction of security while working with tokens in web browser (for example, while using ActiveX components or plug-ins);
  - you don't need to worry about the compatibility of the application with the new browser version.
- It provides the user with a convenient and intuitive graphical interface.
- Deployment using group policy (Microsoft GPO) is available.
- Within the JMS implementation project, it is possible to use the client for Linux and other embedded systems and solutions (M2M, IoT).

Support for Branch Network

- JMS provides the mapping of the users and tokens including their objects to a specific branch, which allows you to track the movement of tokens across the branch network.
- If channel bandwidth between branches and the head office is low JMS servers can work offline, and each of them may be managed from a single console.
- The built-in role-based access control allows you to distribute responsibilities for managing JMS servers among security administrators of the head office and branches of the organization, as well as delegate separate rights to other IT professionals.
- Support for consolidated reports by groups of branches or whole branch network allows you to track the status and usage history of all available tokens.

Minimal Dependency on Microsoft Active Directory (AD)

- You do not need to modify and extend the AD schema (as opposed to competing solutions), because all the necessary data is copied and stored in its own JMS database.
- Apart from AD, other external directory services such as certificate authorities, HR systems, MS SQL databases, FreeIPA, and JDS (JMS's directory service) are supported.

Scalability and Fault Tolerance

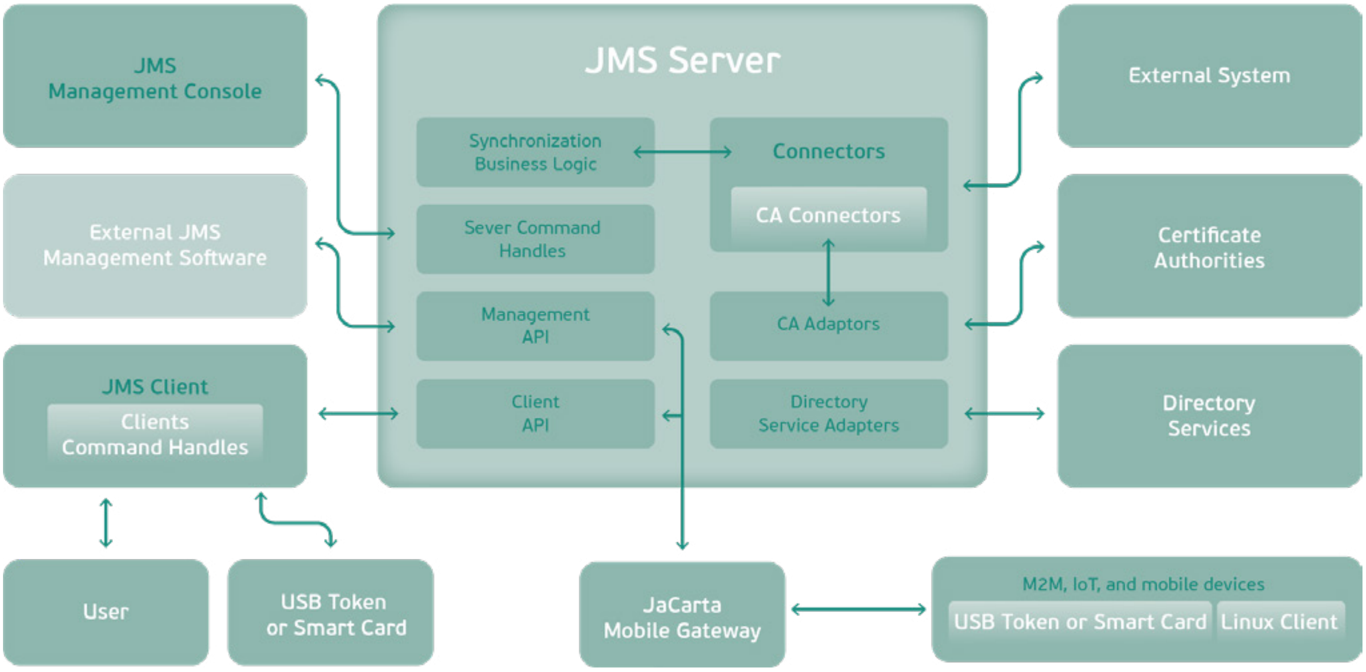
- Virtualization support (VMware ESX and ESXi, Microsoft Hyper-V).
- Support for widespread load balancers.
- Support for cluster technologies (NLB), which provide the following:
  - load balancing between JMS servers when deployed in large organizations;
  - fault tolerance of JMS servers working with a common database (starting with Microsoft SQL Server Standard);
  - disaster recovery is available provided that JMS servers and databases are deployed across different locations (Microsoft SQL Server Enterprise version with AlwaysOn support is recommended).

Safety and Reliability

- The channels between JMS Server and its clients and management console are encrypted using HTTPS (SSL/TLS).
- All critical data are stored in crypto storage requiring access by a digital certificate.
- Implemented a role-based access model may be extended by the authority delegation mechanism.
- The forced user PIN code change is implemented.

JMS Expansion

JMS provides an open server API to expand the system by adding new modules and developing the connectors to certificate authorities (CAs) and external directory services.



- To integrate JMS with an external system in scenarios where the JMS is the lead system, a "connector" is to be developed. Such a connector allows external system to automatically manage the data is to be stored to a token, through the JMS program interface.

- In order to integrate JMS with a new type of CA, it is necessary to develop an "adapter to a CA", which is an extension for the CA connector built into the JMS. The connector to the CA implements the common logic of working with the CA, while the interaction with a specific type of CA is implemented via adapters.

- To integrate JMS with an external directory service, which is the source of user accounts and workstations, you need to develop an adapter to such a service.

Scalability

The table shows the hardware and software requirements depending on the number of JMS users.

Number of Users	Number of Cluster Nodes	JMS Server				SQL Server				JMS -SQL Channel Capacity	MS SQL Server Edition
		CPU		RAM	Disk	CPU		RAM	Disk		
		Cores	GHz	GB	GB	Cores	GHz	GB	GB	Mbps	
<1 000	1	<4	3	4	<100	<4	3	<32	<200	<100	Express / Standard
1 000 – 10 000	2	4-24*	3	4-24*	~100	4-24	3	32–160	200	100-500	Standard
>10 000	2 and more	>24*	3	>24*	>100	>24	3	>160	>200	>500	Enterprise

*The total hardware requirements for all nodes in the cluster are indicated.

Notes

- If the system is to be deployed in several geographically distant branches, the recommendations from the table should be applied for each installation in accordance with the number of users in a particular branch office.
- For any kind of installation, it is recommended to use a fault tolerant DBMS server with a database file on the network storage.

Requirements for Implementation Specialists

JMS implementation specialists should meet the following qualification requirements:

- basic understanding of PKI and its use in the enterprise information systems;
- software installing and configuring skills in Microsoft Windows environment;
- Microsoft network environment (servers, clients, Active Directory) administration skills;
- understanding the features of PKI based on certificate authorities by Entrust, Check Point, Microsoft, CryptoPro, etc.;
- completed JMS training course (desirable).

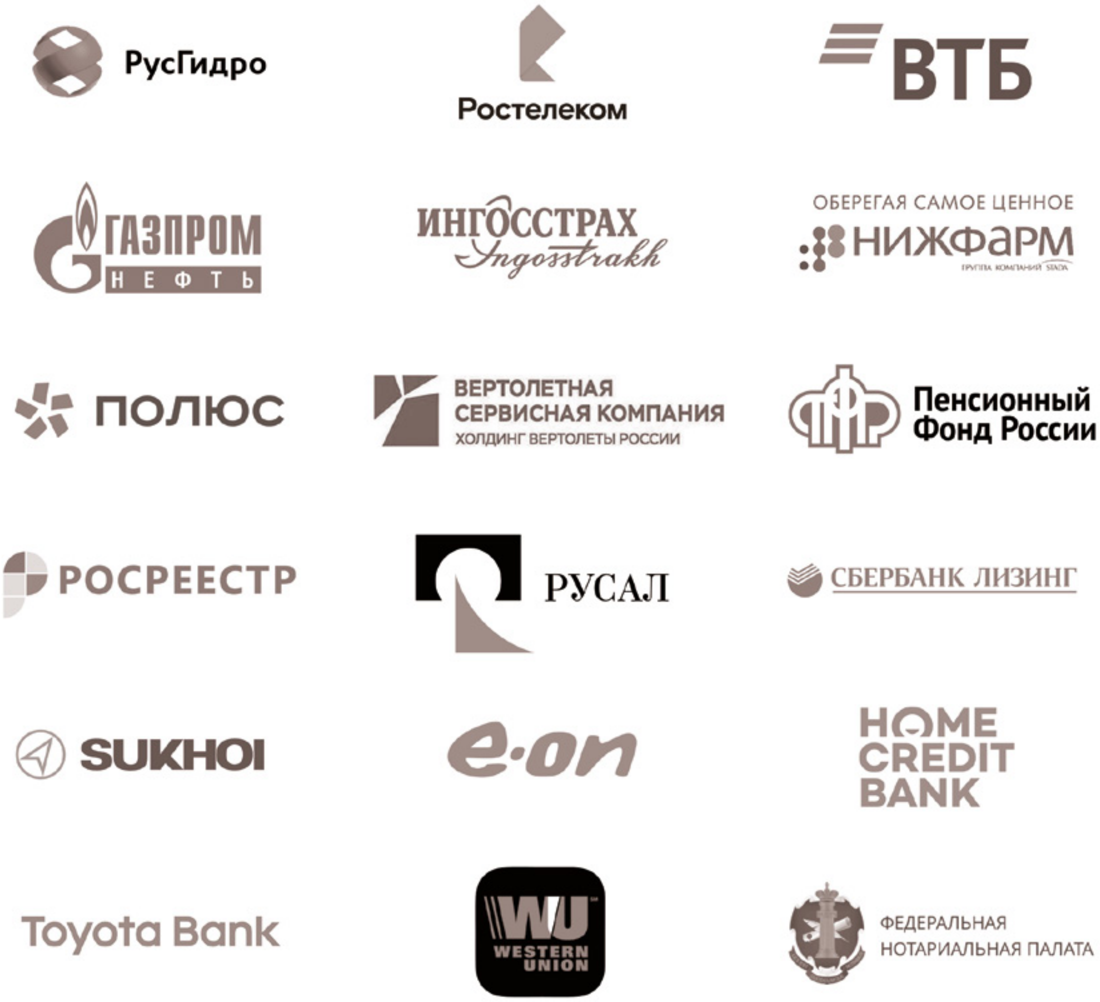
Specifications

Feature	Description		
JMS System Requirements	**Operating System** • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 SP1 • Microsoft Windows Server 2008 SP2	**DBMS** • Microsoft SQL Server 2016 • Microsoft SQL Server 2014 • Microsoft SQL Server 2012 • Microsoft SQL Server 2008	
Workstation System Requirements (JMS Clients, JMS Management Console)	**Microsoft** • Microsoft Windows 10 • Microsoft Windows 8, 8.1 • Microsoft Windows 7 SP1 • Microsoft Windows Vista SP2 • Microsoft Windows XP SP3 (32-bit), SP2 (64-bit) • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 SP1 • Microsoft Windows Server 2008 SP2 • Microsoft Windows Server 2003 R2 SP2 • Microsoft Windows Server 2003 SP2	**Linux** For M2M, IoT, and mobile devices (via JaCarta Mobile Gateway)	
Supported Tokens	**JaCarta** • JaCarta-2 ГОСТ • JaCarta-2 PKI/ГОСТ • JaCarta-2 PKI/BIO/ГОСТ • JaCarta-2 PRO/ГОСТ • JaCarta LT • JaCarta PKI • JaCarta PKI/Flash • JaCarta PRO • JaCarta ГОСТ • JaCarta ГОСТ/Flash • JaCarta PKI/BIO • JaCarta PKI/ГОСТ • JaCarta PKI/ГОСТ/Flash • JaCarta PKI/BIO/ГОСТ • JaCarta PRO/ГОСТ • JaCarta CryptoPro	**eToken** • eToken 5110 • eToken 5105 • eToken 5100 • eToken 4100 • eToken ГОСТ • eToken PRO • eToken PRO (Java) • eToken NG-Flash (Java) • eToken NG-OTP (Java) w/o OTP	**Rutoken** • Rutoken ECP 2.0 • Rutoken ECP • Rutoken S • Rutoken Lite **ESMART** • ESMART Token • ESMART Token ГОСТ **Other** (on demand)
Supported Certificate Authorities	• Entrust Certification Authority* (as part of Entrust Authority Security Manager) • Check Point Internal Certificate Authority* (as part of Security Management Server) • Microsoft CA with CryptoPro CSP • Microsoft CA • CryptoPro CA 2.0	• CryptoPro CA 2.0 • ViPNet CA 4.6 • Notary-PRO 2.7 • Dogtag	
Supported Cryptography Means	Any software and hardware cryptography means		
Supported Directory Services	• Microsoft Active Directory • Microsoft Remote Active Directory • CryptoPro CA 2.0 • CryptoPro CA 1.5 • FreeIPA • JMS native Directory Services (JDS) • Other directory services (require developing of connectors; SDK is provided)		
Scalability	• From 100 to 1,000,000 tokens (using JMS for accounting and managing less than 100 tokens is impractical)		
Virtualization	VMware - ESX - ESXi Microsoft Hyper-V		

* CA connector is in prototype state, but it can be added to release on demand.

Feature	Description
Fault Tolerance and Reliability	• Support for clustering (NLB) • Backing up private keys and certificates
Cross-Border Sales Restrictions	No (There are restrictions only when using certified cryptography means).
Requirements for JMS Distribution Licenses	No (National regulator license is only required when selling tokens with national cryptography on the board, such as JaCarta-2 GOST, eToken GOST, or Rutoken ECP).
Language Localization	• Russian (default) • English • Other (on demand)
Ability to Support Other Type of Tokens	Yes (on demand)

Our Customers



"Aladdin R.D." is a recognized expert and leader in the market of strict two-factor authentication of users in access to corporate resources, web portals and cloud services. Many products, solutions, and technologies of the company are dominating the Russian market and used by leaders of key industries.

For more than 20 years, almost every Aladdin's product has deserved special attention and become the leader in its segment. The products and solutions of Aladdin actually became the corporate standard in many commercial and public organizations.

Aladdin .ru

☎ +7 (495) 223 00 01
✉ aladdin@aladdin.ru
www.aladdin.ru

Specifications are subject to change without notice
All trademarks and trade names are property of their respective owners

More info