

Jrsys

捷而思股份有限公司



Privileged Access Management



Large number of accounts management



Preventing hackers from invading the last line of defense



Automated expired password management system



Winner of International security awards

PAM Jrsys Privileged Access Management

Difficulties in Accounts Management

- Insufficient information staff to handle complicated passwords management for a large number of hosts
- Numerous IT/OT equipment for government and national key information infrastructure, making protection difficult
- When the host manager is not present, operations cannot be carried out or passwords must be lent out for others to handle
- The host operates 24 hours a day, and there is risk for security management for emergency password lending
- Difficulty in controlling password access and inaccurate audit records
- Passwords of multiple groups of account can be easily forgotten, lost, or stolen
- The management administrative process is complex and unable to cope with temporary needs
- Potential concerns for outsourcing manufacturers owning management accounts
- Sharing management accounts with multiple people makes it difficult to clarify the responsibility for incidents
- Difficult to detect hacker's privilege escalating



Privileged Account Management and Audit Best Solution



PAM goal: To improve the efficiency and security of password change and account management, reduce human intervention, and adopt automatic password change and account inventory in the system, Accelerate password changes and optimize the host account management mechanism.

According to a CERT (Computer Emergency Response Team) survey, in the United States the are up to 86% of internal attacks that come from past or present employees. Many data leaks are carried out through legally authorized accounts, entering the internal enterprise, and attacking important data servers through privilege escalating. Therefore, the first priority for enterprise asset security should start with privileged account management.

Jrsys Privileged Account Management System, is independently developed 100% in Taiwan. For many years, Jrsys has assisted our corporate clients in winning international and Taiwan cyber security Innovation Awards, and recognized both local and internationally.

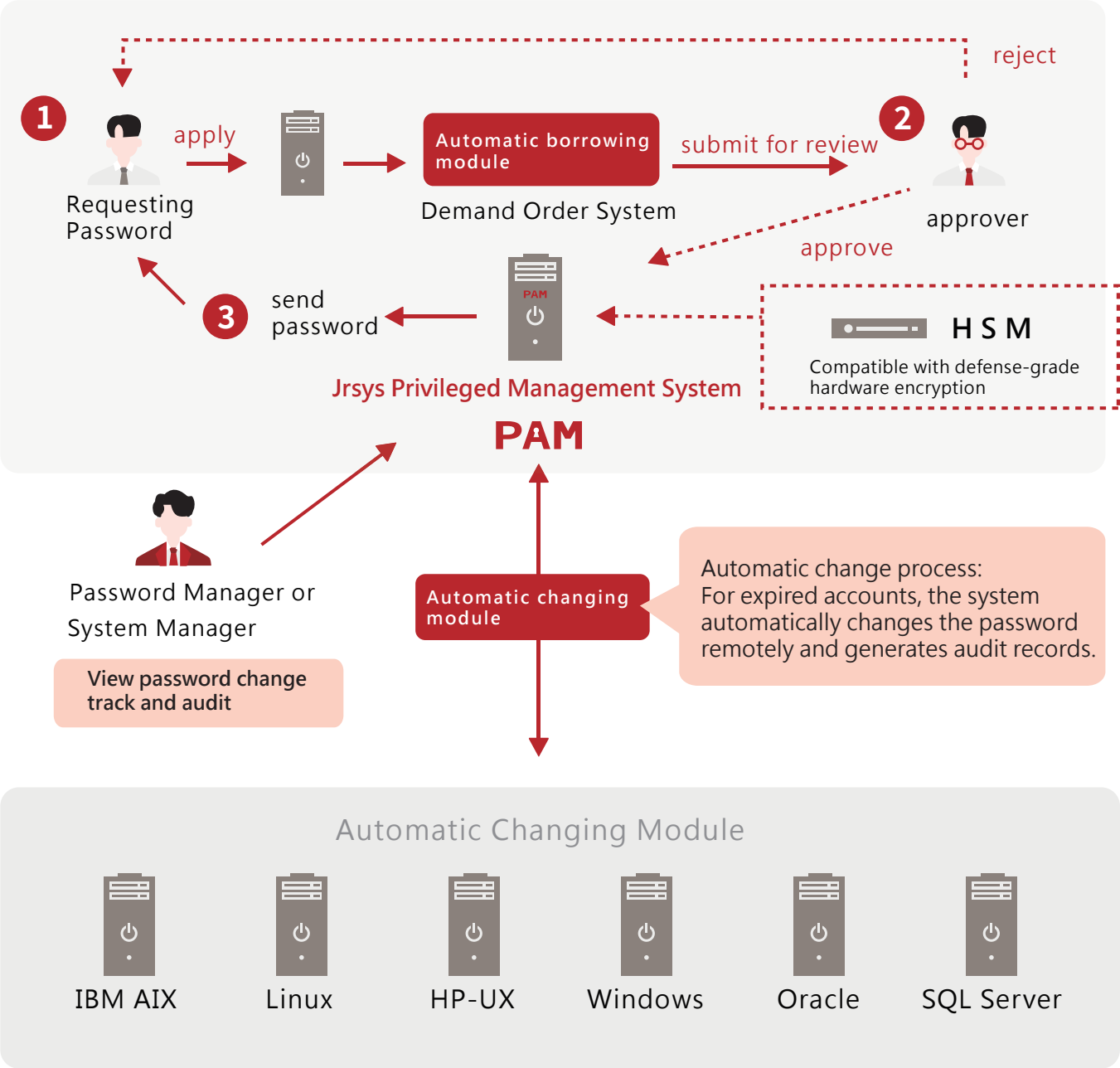
Jrsys has been deeply involved in the field of information security for many years, and has great experience in solving the problems and difficulties faced by enterprises in building internal information. The "Jrsys Privileged Account Management System" can significantly reduce the risk of enterprises abused privileged access accounts, simplify the workflow, support privileged account access management for various IT/OT information platforms, and provide automated operation services such as password change and account inventory taking. Not only can it reduce labor management costs but also improve overall performance.



PAM

Jrsys
捷而思股份有限公司

The Privileged Account Management Structure



Functions

- Change password automatically
- Support batch account import
- Manual/automatic account inventory taking
- Password rules can be adjusted according to needs
- Roles for permission and approval processes
- Provide account requesting, result of change, and audit records
- Built-in application process, which can integrate the demand order system
- Supports online methods such as RDP, Telnet, SSH, HTTP, HTTPS, etc
- Supports various environments, including HP-UX, IBM AIX, Linux, Oracle Solaris, Microsoft Windows, Oracle Database, MS-SQL Server, to meet enterprise usage scenarios

Features

- Capable of supporting defense-grade hardware encryptors (HSM) and multi-factor identity authentication
- Password changes are fully automated and controlled by the system, all data storage and transmission are fully encrypted
- Account inventory and comparison, quickly find unauthorized accounts and ghost accounts, and strictly prevent hackers from claiming rights
- Developed in Taiwan, a quick and convenient request, review, and audit flow to meet customer needs

Password automation management

Step 1

Application for borrowing account and password

User request account and password to access host resources.

Step 2

Audit authorization

Email to notify supervisor for approval.

Step 3

Send password

The system sends a one-time password to the requester.

Step 4

Authorization operation

Users can gain access within the duration allowed.

Step 5

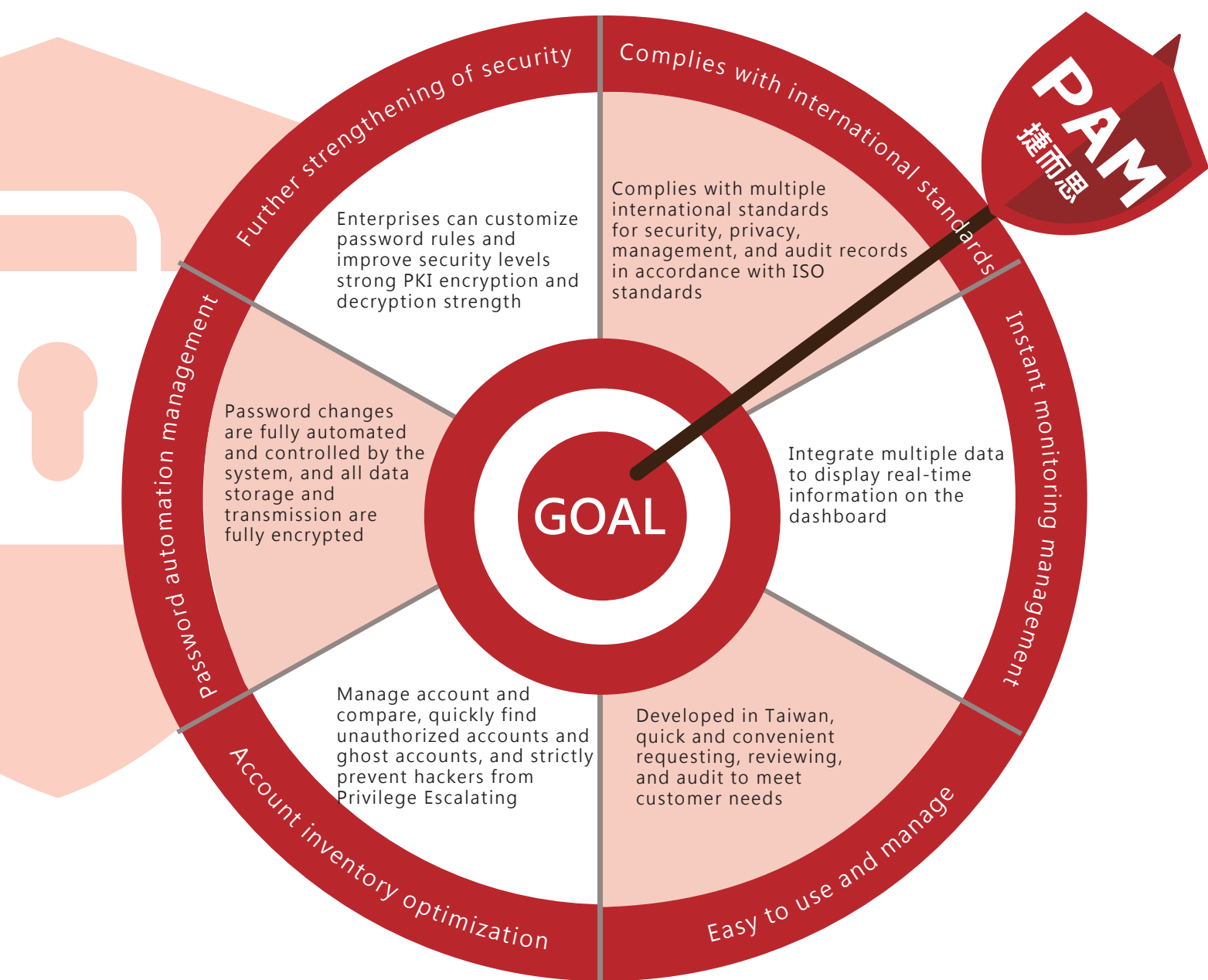
Update password

When the application time expires, the system automatically reset password.



— Applicable industries —

Government units, CIIP (National Key Information Infrastructure Protection), financial holding company, property insurance, securities, investment trust, and industries that require a large amount of accounts management



捷而思股份有限公司

4F., No. 69, Jilin Rd., Zhongshan Dist.,
Taipei City 104, Taiwan (R.O.C.)
(台北市中山區吉林路 69 號 4 樓)

Tel : 02-2511-7131



Facebook Page



Line