IBM Tivoli Key Lifecycle Manager

Simplify, centralize and strengthen encryption key management for your enterprise

Highlights

- Simplify, centralize and automate the encryption key management process
- Enhance data security and help facilitate compliance management of regulations and standards such as the Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley and the Health Insurance Portability and Accountability Act (HIPAA)
- Enhance flexibility with support for the new encryption key management—the Key Management Interoperability Protocol V1.0 (KMIP) from the OASIS standards group

Business data is growing at exponential rates, and along with that growth comes a demand for securing that data. Enterprises have responded by implementing encryption at various layers—in the hardware, on the network and in various applications. This response has resulted in a series of encryption silos—some of it holding confidential customer data—with fragmented approaches to security, keys and coverage.

Different applications across the enterprise often employ different methods of encryption. Some departments in the organization may use public-key cryptography while others use secret-key or hashes. Still others don't encrypt data while it's at rest (such as when it is stored on a device or in a database) but only when the data is in motion, using virtual private networks (VPNs) to secure the data pipeline.

Key management for these encryption approaches is often similarly fragmented. Sometimes key management is carried out by department teams using manual processes or embedded encryption tools. Other times, the key management function is centrally managed and executed. In some cases, there is no formal key management process in place. This fragmented approach to key management can leave the door open for loss or breach of sensitive data.

Deploy a simple solution to a complex problem

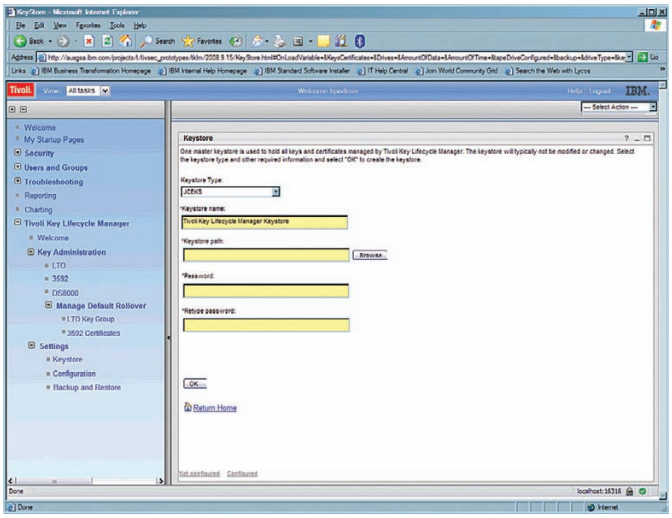
IBM Tivoli® Key Lifecycle Manager provides a simple solution to the complex problem of key management. Traditionally, the more encryption you deploy, the more keys you have to manage. And these keys have their own life cycles, separate from the data they're protecting—and that life cycle has to be managed, from initialization and activation

through expiration and destruction. Tivoli Key Lifecycle Manager can help you better manage the encryption key life cycle, allowing you to simplify, centralize, and strengthen your organization's key management processes and reduce operational costs.

Together with IBM's innovative self-encrypting storage offerings, Tivoli Key Lifecycle Manager offers customers a proven solution that can address their concerns when a tape cartridge or disk drive is removed from the storage system and transported in-house or off-site. Lost storage media is not uncommon these days and brings with it enormous direct and indirect costs for those who lose sensitive information. With IBM System Storage® self-encrypting offerings and Tivoli Key Lifecycle Manager, customers no longer have to worry about losing sensitive information should tapes gets misplaced or stolen. Additionally, support for the new standard KMIP allows IBM Tivoli Key Lifecycle Manager to manage encryption keys for not only IBM self-encrypting storage devices but also a number of non-IBM encryption solutions, hence allowing you to efficiently management encryption keys for your enterprise.

Centrally manage encryption keys

Tivoli Key Lifecycle Manager serves keys at the time of use to allow for centralized storage of key material in a secure location, a unique approach that supports multiple protocols for key serving and manages certificates as well as symmetric and asymmetric keys. Users can also centrally create, import, distribute, back up, archive and manage the life cycle of those keys and certificates using a customizable graphical user interface (GUI).



IBM Tivoli Key Lifecycle Manager provides a wizard to guide administrators through the keystore configuration process.

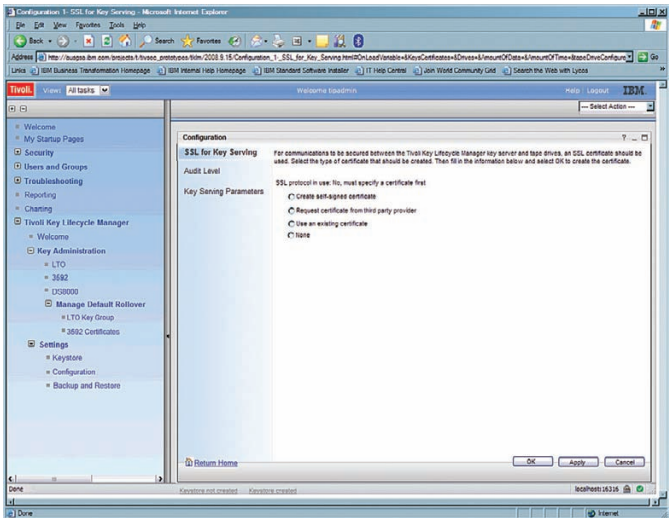
Tivoli Key Lifecycle Manager's transparent encryption implementation means that keys are generated and served from a centralized location and are never sent or stored "in the clear." The embedded encryption engine in the IBM self-encrypting tape offerings encrypt and decrypt the data as it enters and leaves the drive at native tape speeds, which means both faster and more secure handling of data.

Tivoli Key Lifecycle Manager enables customers to group devices into separate domains for improved and simplified management. It allows multiple administrators with different roles and permissions to be defined. Also, by default, the groups of devices only have access encryption keys defined within their group. These role-based access control features enable separation of duties, mapping of permissions for what actions against which objects, and enforcement of data isolation and security in a multitenancy environment. This also enhances security of sensitive key management operations.

Enable strong authentication, strong security

These rich capabilities are made possible by strong authentication between IBM storage systems and Tivoli Key Lifecycle Manager. The drives are manufactured with a built-in unique certificate. When the drives are mounted, information about the hardware serial number and environment is digitally signed by the drive and then sent to the centralized manager, which in turn validates the signature on the generated key pair through the certificate authority.

The final step in the process happens when Tivoli Key Lifecycle Manager checks to make sure the device is valid by verifying that it exists in the drive table. Any unknown device is rejected or placed into a queue to be approved by the administrator. With this strategy, a rogue device cannot be deployed on the network and used to intercept organizational data.



Tivoli Key Lifecycle Manager provides step-by-step screens to help administrators set security options.

In addition to strong authentication, there is also strong security between the storage device and Tivoli Key Lifecycle Manager. The software generates a session key using the generated key pair from the storage device. Using a pre-generated key, the software then sets an encryption key to be used for an individual cartridge on the storage device. Finally, the software wraps the encryption key with the session key and returns the key to the device.

This approach to encryption can dramatically increase data security while simplifying encryption key management. Users don't need to know anything about encryption in order to realize the benefits. Administrators can easily manage a smaller set of more secure keys. And performance isn't impacted because each storage device has hardware built into it that performs at wire speed without latency. Not having to change other processes, install more hardware, or reconfigure software to support it means that the security is kept simple and straightforward.

Leverage flexible implementation options

Tivoli Key Lifecycle Manager can be applied at different levels to simplify key management while meeting the unique needs of your organization.

- For organizations that manage keys within separate silos, Tivoli Key Lifecycle Manager can simplify complex key distribution and management, reducing administrative burdens within each silo.
- For organizations that want centralized control and policy-driven key management, Tivoli Key Lifecycle Manager offers consolidated management of keys across domains, supports standards that extend management to both IBM and non-IBM products, and integrates well into existing security team methodologies.
- For organizations taking a hybrid approach, such as centralized management for storage only, Tivoli Key Lifecycle Manager can make compliance reporting much easier, and can enhance key backup and recovery processes in case of disaster. This approach also enables organizations to establish administrative access based on roles—in this case, storage security.

Simplify key configuration and management tasks

Tivoli Key Lifecycle Manager provides an easy-to-use, web-based GUI that helps simplify key configuration and management tasks. With this GUI, administrators can easily create keystores, assign keys and certificates, and manage the life cycle of both from a centralized console.

The software itself is typically installed on your most secure and highly available server or dedicated workstation. Once installed, the GUI allows administrators to perform basic local key life cycle management on the drives, and offers not only configuration and setup tools, but also audit and compliance support. The software provides three ways to add encryption-enabled devices: Auto-discovery of encryption-capable devices, discovery with administrator's approval or manual addition. Once added, default keys are assigned.

The GUI also allows administrators to implement key retention for backed-up data and to address rules for regulatory compliance and legal discovery. In case of disaster, the administrator can provide a set of keys that can unlock encrypted backups and make them available for use again. The administrator can configure rules for automated rollover of certificates or groups of keys so that new encryption keys are used automatically based on a configurable schedule. In this way, administrators can limit the amount of data which is encrypted with particular keys, minimize exposure when a key is compromised, and facilitate erasure of data by deleting relevant keys when data is set to expire.

Achieve quick time to value with wizard-based assistance

Tivoli Key Lifecycle Manager uses a wizard-based guide to help administrators through a series of simple, task-based screens. The first task is to create a keystore, which is then used to hold all the keys and certificates managed by Tivoli Key Lifecycle Manager. To configure a keystore, the administrator enters relevant information about it into the system, such as its name, the keystore type, the path where it will be stored, and its password.

Once the keystore is created, the administrator can configure different devices to use certain communication protocols including Key Management Interoperability Protocol. For example, for secure communications between Tivoli Key Lifecycle Manager and a drive, the administrator can create a self-signed SSL certificate, request a certificate from a third-party provider, or use an existing certificate. The ability to use any of these options gives the administrator the power to work within an existing security policy or set of procedures, or respond quickly to local conditions.

Administrators also have the option of setting the audit level (from low to high) and setting other key serving parameters, such as TCP port, SSL port and timeouts.

Once the SSL configuration is complete, devices can be added to the system. The devices appear in the Tivoli Key Lifecycle Manager Key Administration and are ready for use as a secure storage endpoint. The keys associated with the device can then be managed through the GUI, including making updates, expiring or destroying the keys. The Tivoli Key Lifecycle Manager Key Administration Welcome Page provides critical notices to the administrator including information about last backups, available protocols, and notices of expiring certificates.

Deploy a unified key management strategy

Tivoli Key Lifecycle Manager enables a unified key management strategy that can help better secure your data, with performance you need to support your critical business functions. Built on open standards, including Key Management Interoperability Protocol, the solution enables flexibility and facilitates vendor interoperability. Its intuitive interface enables quick time to value, while its innovative approach can help dramatically reduce the number of keys administrators have to manage. By enabling centralized management of strong encryption keys throughout the key life cycle, Tivoli Key Lifecycle Manager can help minimize the risk of exposure as well as helping to reduce operational costs.

For more information

To learn more about IBM Tivoli Key Lifecycle Manager, contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/tivoli/products/key-lifecycle-mgr

About Tivoli software from IBM

Tivoli software offers a service management platform for organizations to deliver quality service by providing visibility, control and automation—visibility to see and understand the workings of their business; control to effectively manage their business, help minimize risk and protect their brand; and automation to help optimize their business, reduce the cost of operations and deliver new services more rapidly. Unlike IT-centric service management, Tivoli software delivers a common foundation for managing, integrating and aligning both business and technology requirements. Tivoli software is designed to quickly address an organization's most pressing service management needs and help proactively respond to changing business demands. The Tivoli portfolio is backed by world-class IBM Services, IBM Support and an active ecosystem of IBM Business Partners. Tivoli clients and Business Partners can also leverage each other's best practices by participating in independently run IBM Tivoli User Groups around the world—visit www.tivoli-ug.org

IBM Corporation Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
September 2010

Tivoli software

TID14031-USEN-01