Planning

Contents

Planning

Planning is an activity in which your decisions affect one or more subsequent activities.

Activities include tasks such as planning the key size and database requirements, and determining ongoing working practices that your site requires.

Site requirements

Before you install IBM Security Key Lifecycle Manager, consider site issues such as your requirements for key size, whether to use the DB2® that IBM Security Key Lifecycle Manager provides, or an existing copy that is already installed on your system.

Key size requirements

You must consider the requirements for key sizes before you install and configure IBM Security Key Lifecycle Manager.

Supported key sizes and import and export restrictions

IBM Security Key Lifecycle Manager can serve either 2048 or 1024-bit keys to devices. Older keys that were generated as 1024-bit keys can continue to be used.

Table 1 lists the supported key sizes that IBM Security Key Lifecycle Manager supports.

Table 1. Supported key sizes

Import PKCS#12 file	Export PKCS#12 file	Key Generation Size in Bits
Yes	Yes	2048

DB2 planning

You must consider whether to use an existing copy of DB2 Advanced Workgroup Server Edition, or use the DB2 version and fix pack that the IBM Security Key Lifecycle Manager installation program provides for distributed systems. An existing DB2 must be locally installed on the system and not on a network or shared drive.

Use IBM Security Key Lifecycle Manager to manage the DB2.

IBM Security Key Lifecycle Manager requires DB2 Advanced Workgroup Server Edition, Version 11.10 and the future fix packs on the same system on which the IBM Security Key Lifecycle Manager server runs.

Note:

- You must use IBM Security Key Lifecycle Manager to manage the database. To avoid data synchronization problems, do not use tools that the database application might provide.
- For improved performance of DB2 Version 11.10 on AIX systems, ensure that you install and configure the I/O completion ports (IOCP) package that is

described in the DB2 documentation (http://www-01.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.admin.perf.doc/doc/t0054518.html).

- If an existing copy of DB2 Advanced Workgroup Server Edition was installed as the root user at the correct version for the operating system, you can use the existing DB2 Advanced Workgroup Server Edition. IBM Security Key Lifecycle Manager installer does not detect the presence of DB2. You must specify the DB2 installation path.

For more information on database requirements, see the "Installing and configuring" section on IBM Knowledge Center for IBM Security Key Lifecycle Manager.

Certificate requirement to encrypt data

IBM Security Key Lifecycle Manager requires at least one `X.509` digital certificate, which contains a public/private key pair, to protect the data encryption key that IBM Security Key Lifecycle Manager server creates when data encrypts on 3592 tape drives or DS8000 Turbo drives.

IBM Security Key Lifecycle Manager allows for two- digital certificate aliases to be defined per write request. One of the two aliases (labels) specified must have a private key in the IBM Security Key Lifecycle Manager keystore database when the tape or disk is created. This key enables the creator to read the tape or disk. The other alias (label) can be a public key from a partner, which the partner is able to decrypt with its private key. To read an encrypted tape or disk, the correct private key is needed.

There are two methods of setting up digital certificates:

- Create your own public/private key pair and corresponding certificate to be used to write and encrypt to tape or disk fort you to read and decrypt the data later.
- Obtain a public key and corresponding certificate from a partner to be used to write and encrypt tapes or disks that can be read and decrypted by your partner.

Tape sharing with other organizations

You can share tapes with other organizations for data transfer, joint development, contracting services, or other purposes. The methods for sharing encrypted tapes differ for 3592 tape drives and LTO tape drives.

If you move keys to your own disaster recovery location, use a keystore database. If you move keys to a business partner, provide a public key to the business partner.

Verify the validity of any certificate that is received from a business partner by checking the chain of trust of such a certificate back to the certificate authority (CA) that ultimately signed it. If you trust the CA, then you can trust that certificate. Alternatively, validity of a certificate can be verified when it was securely guarded during transfer. Failure to verify a certificate's validity in one of these ways might open the door to a "Man-in-the-Middle" attack.

3592 tape sharing

IBM Security Key Lifecycle Manager can store two sets of wrapped encryption keys on a 3592 tape. This practice allows another organization to read that specific tape without providing them any shared secret information or compromising the security of your certificates and keys.

Add the public part of the public/private certificate of the other organization, and keys to the keystore database of your IBM Security Key Lifecycle Manager, by using a second alias (or key label). When the tape is written, the encryption keys are stored on the tape, which is protected by two sets of public/private keys that are your set and the set that belongs to another organization. The other organization must have an encryption-enabled 3592 tape drive. The other organization can use its IBM Security Key Lifecycle Manager and its private key to unwrap the data key that allows reading that specific tape.

Your IBM Security Key Lifecycle Manager must have the certificate of the partner organization. The other organization must have the associated private key in the keystore that is used by the IBM Security Key Lifecycle Manager that the other organization runs. This flexibility provides tapes that are readable by both organizations. If you want to take advantage of this capability you must add the certificate of the other organization, which contains the public key, to your keystore database.

LTO tape sharing

To share encrypted data on an LTO tape, a copy of the symmetric key that is used to encrypt the data on the tape must be made available to the other organization. This key enables them to read the tape. To share the symmetric key, the other organization must share their public key with you.

This public key is used to wrap the symmetric key when it is exported from the IBM Security Key Lifecycle Manager keystore. When the other organization imports the symmetric key into their IBM Security Key Lifecycle Manager keystore, it is unwrapped by using their corresponding private key.

This practice ensures that the symmetric key is safe in transit since only the holder of the private key can unwrap the symmetric key. With the symmetric key that was used to encrypt the data in their IBM Security Key Lifecycle Manager keystore, the other organization can then read the data on the tape.

Suggested site practices

Planning for an encryption key server such as IBM Security Key Lifecycle Manager must consider site practices that can range from first-time implementation to well-established practices.

Table 2 is a list of best practices that your site might consider.

Table 2. Suggested site practices

Topic	Suggested Practice
Self-signed certificates	Use self-signed certificates for internal production and test purposes within a company.
CA-issued certificates	For a production environment, use CA-issued certificates.
Frequency of certificate replacement	On a quarterly basis, replace certificates that are used to create new cartridges.

Table 2. Suggested site practices (continued)

Topic	Suggested Practice
Minimum number of CA-issued certificates	One certificate is the minimum, and assumes that the certificate is used both as the default and partner certificate.
Normal quantity of tape drives in test and production environments	Quantity ranges from several devices to several hundred, with the median number of devices in the 100+ range.
Remote sites	One or more remote sites exist, and IBM Security Key Lifecycle Manager serves keys to the remote sites.
Number of compromised certificates that occur annually	Zero certificates are compromised.
Mandatory failover requirement	Many sites require that a backup encryption key server must always be running at another site. The primary site makes a backup of the key materials whenever the data changes. Additionally, backed-up data is dependably restored to the offsite replica IBM Security Key Lifecycle Manager server for use in the event of a failover.
Selectively encrypt or encrypt all data	You must consider whether to selectively encrypt or encrypt all data except the keystore database, and recovery issues that might arise. A large percentage of sites encrypts all data, except the IBM Security Key Lifecycle Manager data and its backup data.
Backup files	For more information, see administration topics on backup and restore.
Replication	For more information, see administration topics on replication configuration.

Self-signed certificates

You must consider how to balance the availability of self-signed certificates against the security needs of your enterprise.

Determine your organization's policy on the use of self-signed and certificates that are issued by a certificate authority (CA). You might need to create self-signed certificates for the test phase of your project. In advance, you might also request certificates from a certificate authority for the production phase.

Security for sensitive information

You must ensure that only authorized persons can gain access to sensitive information for IBM Security Key Lifecycle Manager key materials in the IBM Security Key Lifecycle Manager database.

Sites vary in their separation of duties, and might have no separation of duties. However, for greater security, a site can take these steps:

- One person provides runtime system administrator support for the IBM Security Key Lifecycle Manager server. The site has a system administrator to run the IBM Security Key Lifecycle Manager server.
- A different person serves as database administrator, with restricted access to the DB2 user ID and database instance that IBM Security Key Lifecycle Manager uses.

Secure configurations

You must maximize security in environment, installation, administration, and operations to ensure that only authorized persons can gain access to sensitive information for IBM Security Key Lifecycle Manager.

Environment

You can configure these environmental elements for maximum security:

- Restrict physical access to systems to prevent unauthorized access to the server hardware, allowing only authorized administrators to have access to the system console.
- Ensure that the communication network is secure against eavesdropping and spoofing.
- Use a firewall and maintain all ports behind the firewall. Open only the ports that IBM Security Key Lifecycle Manager requires.
- Specify file system controls to protect sensitive files on the IBM Security Key Lifecycle Manager system. Controls must secure the files and limit access to only those users who require access.
- Secure the key server, configuration files, log files, audit log file, database instance, and IBM Security Key Lifecycle Manager backup files.
- Ensure that the system has adequate disk space to store the audit logs.
- If you use any kind of debugging utility on IBM Security Key Lifecycle Manager, you must ensure that the output is secure. Access IBM Security Key Lifecycle Manager only from a secure system in which you are aware of all installed applications.
- Although sensitive information in the IBM Security Key Lifecycle Manager backup JAR file is protected by password, not all of the contents of the JAR file is protected by password, making the file vulnerable to corruption or intentional damage. Keep the JAR file secure.
- Do not edit the files that are contained in a backup JAR file. The files become unreadable. Retain backup files in a secure location to which you control the password. Retain a copy of backup files in a secure location that is not on the IBM Security Key Lifecycle Manager computer, and not in the IBM Security Key Lifecycle Manager directory path.
- When you use a browser to administer IBM Security Key Lifecycle Manager, by using some of the IBM Security Key Lifecycle Manager panels, you can browse the directory layout on the server system. IBM Security Key Lifecycle Manager as a product runs as root, and when you browse the file system, these root permissions are used.

Installation

- Do not install on a domain controller.
- Do not install on a shared file system.

Administrative and user assumptions

Securely manage administrators:

- Grant administrator rights only to persons who manage IBM Security Key Lifecycle Manager and who meet your site requirements for trust and competence in maintaining the security of IBM Security Key Lifecycle Manager.
- Administrators must work in accordance with the guidance provided by the system documentation and IBM Security Key Lifecycle Manager documentation.

- The SKLMAdmin is a privileged user with unrestricted access to IBM Security Key Lifecycle Manager. A user must log in as SKLMAdmin only when the privilege is required.
- The WebSphere® Application Server administrator is a privileged user with access to create user accounts and grant access to IBM Security Key Lifecycle Manager. Provide the WASAdmin user ID and password only to authorized persons.
- Grant user IDs on the system only to users authorized to work with the information on the systems.
- Ensure that users with access to IBM Security Key Lifecycle Manager are cooperative and not hostile.
- Do not grant operating system privileges to administrators such as LTOAuditor who is not required to start or stop the IBM Security Key Lifecycle Manager server.

Operation

Securely manage ongoing operation:

- Enable the suggested password policy.
- Choose and manage the user and administrator passwords according to the password policy.
- Enable auditing.
- Establish and implement the necessary procedures for the secure operation of the system.
- Ensure that maintenance procedures include regular diagnostics and auditing of the system, including regular backups and review of the audit files and error logs.
- Transmit passwords securely to system users.
- Instruct users and administrators to not disclose their passwords.
- There is no lockout mechanism for users who repeatedly enter incorrect passwords.
- Protect the configuration file from disclosure as rigorously as the administrator password itself, including all representations of the content of the configuration file, such as printouts and backups.

Configuration properties and attributes

Table 3 describes a set of configuration properties and attributes with settings for maximum security. Configure a property in a way that is secure, but not set for maximum security. These examples are provided to help you understand those decisions.

Table 3. Secure configuration property settings

Property	Most secure recommendation
Audit.event.outcome	Specify success and failure events.
Audit.eventQueue.max	Set to a value of zero.
Audit.event.types	Specify all values other than the value none.
Audit.handler.file.multithreads	No security impact.
Audit.handler.file.name	Specify a valid, secure location for the file.
Audit.handler.file.size	No security impact.

Table 3. Secure configuration property settings (continued)

Property	Most secure recommendation
Audit.handler.file.threadlifespan	No security impact.
backup.keycert.before.serving	Set to a value of `true`.
cert.valiDATE	Set to a value of `true`.
config.keystore.name	Do not change this value.
config.keystore.ssl.certalias	Use the graphical user interface or the command-line interface to set the valid value for the protocol.
debug	Enabling debug logging might affect IBM Security Key Lifecycle Manager performance. Enable this option only under the guidance of your IBM support representative.
device.AutoPendingAutoDiscovery (an attribute in the IBM Security Key Lifecycle Manager database)	Set to a value of `0` (zero, or manual) or `2` (auto pending).
enableClientCertPush	Set to a value of `false`.
enableMachineAffinity (an attribute in the IBM Security Key Lifecycle Manager database)	Set to a value of `true` (enabled).
fips	Set to a value of `true` (enabled).
KMIPListener.ssl.port	Set to a valid port number.
lock.timeout	Use the default value.
maxPendingClientCerts	Use the default value.
pcache.refresh.interval	Use the default value.
tklm.backup.db2.dir	Specify a valid, secure directory.
tklm.backup.dir	Specify a valid, secure directory.
tklm.encryption.keysize	Use the default value.
tklm.encryption.password	This property is internally used. Do not change its value.
tklm.lockout.attempts	Use the default value.
tklm.lockout.enable	Set to a value of `true` (enabled).
tklm.encryption.pbe.algorithm	This property is internally used. Do not change its value.
TransportListener.tcp.port	Specify a valid port number.
TransportListener.tcp.timeout	Specify a valid timeout interval.
TransportListener.ssl.ciphersuites	Use the default value.
TransportListener.ssl.clientauthentication	Specify the highest value that your device supports.
TransportListener.ssl.port *	Specify a valid port number.
TransportListener.ssl.protocols	Specify a value of `SSL_TLSv2`.
TransportListener.ssl.timeout	Specify a valid timeout interval.
Transport.ssl.vulnerableciphers.patterns	Use the default value.
stopRoundRobinKeyGrps	Specify a value of `true`, although in some environments `false` might be acceptable. For more cautions, see the reference topic for the **stopRoundRobinKeyGrps** property.
useSKIDefaultLabels	No security impact.
zOSCompatibility	No security impact.

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law :

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not

been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at http://www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Index

Numerics

A

B

C

D

E

F

I

K

L

M

O

P

R

S

T

U

V

Z