Glossary

Contents

Glossary

The glossary includes terms and definitions related to IBM Security Key Lifecycle Manager.

Glossary

To view glossaries for other IBM products, see http://www-01.ibm.com/software/globalization/terminology/.

A

AES Advanced Encryption Standard. A data encryption technique that improved upon and officially replaced the Data Encryption Standard (DES).

alias See key label.

authentication
A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures. See also authorization.

authorization
The process of granting a user either complete or restricted access to an object, resource, or function. See also authentication.

C

certificate
In computer security, a digital document that binds a public key to the identity of the certificate owner, enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority.

certificate Authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate.

certificate label
See key label.

challenge
A request for certain information to a system. The information, which is sent back in response to this request, is necessary for authentication.

cipher suite
The combination of authentication, key exchange algorithm, and the TLS cipher specification that is used for the secure exchange of data.

cluster
A collection of independent systems (nodes) that are organized into a network for sharing resources and communicating with each other.

command-line interface (CLI)
A computer interface in which the input and output are text-based.

cryptography
A method for protecting information by transforming it (encrypting it) into an unreadable format, called ciphertext. Only users who possess a secret key can decipher (or decrypt) the message into plain text.

CSV file
A common type of file that contains data that you can separate by commas.

D

data key
An alphanumeric string that is used to encrypt data.

digital certificate
An electronic document that identifies an individual, server, company, or some other entity. A digital certificate associates a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority. See also "certificate authority".

data source
The source of data itself, such as a database or XML file, and the connection information necessary for accessing the data.

E

ECDSA
Elliptic Curve Digital Signature Algorithm. A system for asymmetric, public-key cryptography that is used for encryption and authentication. This algorithm uses elliptic curve cryptography to provide a variant of the Digital Signature Algorithm.

encryption
The conversion of data into a cipher. A key is required to encrypt and decrypt the data. Encryption provides protection from persons or software that attempt to access the data without the key.

externally encrypted data key
A data key that is encrypted (wrapped) by a key encryption key before you store it in the data cartridge. See key encrypting key.

F

failover
An automatic operation that switches to a redundant or standby system in the event of a software, hardware, or network interruption.

failback
In high availability disaster recovery, the process of restarting the original primary system and returning it to its status of primary system after a failover has occurred.

H

Hardware Security Module (HSM)
A hardware security module (HSM) is a device that provides secure storage to store cryptographic keys.

Hypertext Transfer Protocol (HTTP)
An Internet protocol that is used to transfer and display hypertext and XML documents on the web.

Hypertext Transfer Protocol Secure (HTTPS)
An Internet protocol that is used by web servers and web browsers to transfer and display hypermedia documents securely across the Internet.

J

JAR file
A Java archive file.

JavaScript Object Notation (JSON)
A lightweight data-interchange format that is based on the object-literal notation of JavaScript. JSON is programming-language neutral but uses conventions from various languages.

JDBC (Java Database Connectivity)
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call-level API for SQL-based database access.

K

key encrypting key
An alphanumeric, asymmetric key that is used to encrypt the data key. See externally encrypted data key.

key label
A unique identifier that is used to match the externally encrypted data key with the private key that is required to unwrap the protected symmetric data key.

Key Management Interoperability Protocol (KMIP)
Key Management Interoperability Protocol (KMIP) is a communication protocol between a key management server and an encryption system. The KMIP standard is developed by the KMIP technical committee Organization for the Advancement of Structured Information Standards (OASIS).

key ring
In computer security, a file that contains public keys, private keys, trusted roots, and certificates.

keystore
A database of private keys and their associated X.509 digital certificate chains that are used to authenticate the corresponding public keys. In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted, or public, keys.

L

LDAP (Lightweight Directory Access Protocol)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

LDAP directory
A type of repository that stores information on people, organizations, and other resources and that is accessed by using the LDAP protocol. The

entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

lifecycle
Passage or transformation through different stages over time. For example, markets, brands, and offerings have lifecycle.

lifecycle rules
A set of rules in a policy that determine which operations to use when automatically handling commonly occurring events, such as suspending an account that is inactive for a period.

M

migration
The movement of data when the software is upgraded or the data is transferred to a different hardware system or model.

N

node A node is a computer system that is a member of a cluster.

P

password
In computer and network security, a specific string of characters that is used by a program, computer operator, or user to access the system and the information that is stored within it.

policy A set of considerations that influences the behavior of a managed resource or a user.

private key
In secure communication, an algorithmic pattern, which is used to encrypt messages that only the corresponding public key can decrypt. The private key is also used to decrypt messages that were encrypted by the corresponding public key. The private key is kept on the user's system and is protected by a password.

public key
The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures or decrypt data that is encrypted with the corresponding private key.

R

rekey The process of changing the asymmetric Key Encrypting Key that protects the Data Key that is stored on an already encrypted tape, allowing different entities access to the data.

replication
The process of maintaining a defined set of data in more than one location. Replication involves copying designated changes for one location (a source) to another (a target) and synchronizing the data in both locations.

Representational State Transfer (REST)
A software architectural style for distributed hypermedia systems like the World Wide Web. The term is also often used to describe any simple

interface that uses XML (or YAML, JSON, plain text) over HTTP without an additional messaging layer such as SOAP.

response file
A file that can be customized with the setup and configuration data that automates an installation. During an interactive installation, the setup and configuration data must be entered, but with a response file, the installation can proceed without any intervention.

RSA Rivest-Shamir-Adleman algorithm. A system for asymmetric, public-key cryptography that is used for encryption and authentication. The security of the system depends on the difficulty of factoring the product of two large prime numbers.

rule A condition that is used in the evaluation of a policy.

S

Secure Socket Layer (SSL)
A security protocol that provides communication privacy. SSL enables client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

security
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

SSL handshake
A Secure Sockets Layer (SSL) session always begins with an exchange of messages called the SSL handshake. The handshake allows the server to authenticate itself to the client by using public key techniques, and then allows the client and the server to cooperate in the creation of symmetric keys that are used for rapid encryption, decryption, and tamper detection during the session that follows.

syslog A standard for transmitting and storing log messages from many sources to a centralized location to enhance system management.

system administrator
An individual who is responsible for the configuration, administration, and maintenance of a computer system or application.

T

Transmission Control Protocol/Internet Protocol (TCP/IP)
An industry-standard, non-proprietary set of communication protocols that provides reliable end-to-end connections between applications over interconnected networks of different types.

Transport Layer Security (TLS)
A set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for authentication purposes in Web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys.

U

Uniform Resource Locator (URL)
The unique address of an information resource that is accessible in a network such as the Internet. The URL includes the abbreviated name of the protocol that is used to access the information resource and the information used by the protocol to locate the information resource.

W

worldwide name
Name of a device such as a tape drive. The worldwide name is a non-secure, 64-bit address that is used in networks to uniquely identify each element. For example, to define devices and device paths, you might combine the value of the worldwide name with a device serial number, and other information of each disk device and tape drive used.

X

X.509 certificate
A certificate that contains information that is defined by the X.509 standard.

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, MD-NC119
Armonk, NY 10504-1785
US

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 jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may 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 Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

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_.

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.