



SURFACE VEHICLE RECOMMENDED PRACTICE

J3201™

SEP2024

Issued

2024-09

Guidelines for Automotive Environment Cybersecurity Key Management and Credential Distribution

RATIONALE

This document provides guidance to the reader for the management and distribution of credential material for the road vehicle. Common use cases are defined in this document and are known as service definitions. There are primary and secondary service definitions, which can serve as the basis for applicable use cases to an original equipment manufacturer (OEM) or a tiered supplier.

This document includes the following:

- Recommended practice guidance on exchange of credentials, within and between OEM and Tier-n suppliers using Key Management Interoperability Protocol (KMIP).
- Support for key and credential types common to the automotive industry
- Support for key provisioning, revocation, and rotation mechanisms.

SAE Executive Standards Committee Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2024 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, or used for text and data mining, AI training, or similar technologies, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER: Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
http://www.sae.org

SAE WEB ADDRESS:

Full document details: SAE J3201_202409

For more information on this standard, visit https://www.sae.org/standards/content/J3201_202409/

Documents

Standard, visit Sharing Hub

TABLE OF CONTENTS

1.	SCOPE.....	4
1.1	Scope of Authority.....	4
1.2	Safety versus Security.....	4
1.3	Development Considerations.....	4
1.4	Purpose.....	4
1.5	How to Use This Document.....	5
1.6	Diagrams.....	5
2.	REFERENCES.....	5
2.1	Applicable Documents.....	5
2.1.1	SAE Publications.....	5
2.2	Related Publications.....	5
2.2.1	ISO Publications.....	5
2.2.2	NIST Publications.....	5
2.2.3	AUTOSAR Publications.....	6
2.2.4	IETF Publications.....	6
2.2.5	Other Publications.....	6
3.	DEFINITIONS AND ACRONYMS.....	7
3.1	Definitions.....	7
3.2	Acronyms.....	22
4.	DOCUMENT CONVENTIONS.....	23
5.	ASSUMPTIONS.....	24
5.1	Overall Key Management.....	24
5.2	Transport and Protection of KMIP Communication and Objects.....	24
5.3	Transport Layer Protection.....	24
5.3.1	Locality of Implementation.....	24
5.3.2	Functionality.....	24
5.4	Object Provisioning Environment.....	25
5.5	Provisioning of Software Signing Keys.....	25
5.6	Root Certificate Authority (CA) for Signing.....	25
5.7	Cybersecurity Best Practices.....	25
5.8	Location of Client/Server.....	25
6.	GOALS AND OBJECTIVES.....	25
7.	RECOMMENDED PRACTICES FOR KEY MANAGEMENT.....	26
7.1	OASIS KMIP Service Profiles.....	26
7.1.1	OASIS KMIP Baseline Server Profile.....	26
7.1.2	OASIS KMIP Baseline Client Profile.....	26
7.1.3	OASIS KMIP Complete Server Profile.....	26
7.2	Service Definitions.....	26
7.2.1	KCMS Environment Provisioning.....	27
7.2.2	Provisioning of Software and Firmware Signing Keys for Build System.....	27
7.2.3	Use of ECU Encryption Keys.....	28
7.2.4	Primary Service Definitions.....	30
7.2.5	Application Service Definitions.....	44
8.	NOTES.....	49
8.1	Revision Indicator.....	49

APPENDIX A	POTENTIAL SERVICE DEFINITIONS	50
APPENDIX B	RATIONALE FOR DESIGN DECISIONS	51
APPENDIX C	RECOMMENDED ATTRIBUTES.....	52
Figure 1	Client associates existing object to ECU type	30
Figure 2	Client registers objects associated with production run batch.....	32
Figure 3	Client asynchronously requests key injection for production run batch of ECUs	33
Figure 4	Server associates injected, managed object to recipient ECU	34
Figure 5	Client asynchronously requests key injection for specifically identified ECU	36
Figure 6	Register feature locking/unlocking codes to server	37
Figure 7	Client obtains status on one or more ECU injection requests	39
Figure 8	Client obtains injection DateTime for ECU in production run batch.....	40
Figure 9	Client associates object to VIN	43
Figure 10	ECU generates its own key pair.....	45
Figure 11	ECU requests intermediate server.....	46
Figure 12	Registering security objects per element.....	47
Table 1	Provisioning of software and firmware signing keys for build system.....	27
Table 2	Use of ECU encryption keys	28
Table 3	Client associates existing object to ECU type	31
Table 4	Client registers objects associated with production run batch.....	32
Table 5	Client asynchronously requests key injection for production run batch of ECUs	33
Table 6	Server associates injected, managed object to recipient ECU	35
Table 7	Client asynchronously requests key injection for specifically identified ECU	36
Table 8	Register feature locking/unlocking codes to server	38
Table 9	Client obtains status on one or more ECU injection requests	39
Table 10	Client obtains injection DateTime for ECU in production run batch.....	41
Table 11	Client associates object to VIN	44
Table 12	ECU generates its own key pair.....	45
Table 13	ECU requests intermediate server.....	46
Table 14	Registering security objects per element.....	47
Table 15	Provisioning security credentials to in-vehicle ECUs.....	48

1. SCOPE

1.1 Scope of Authority

This document specifically pertains to cybersecurity for road vehicles. This document encompasses the entire vehicle lifecycle of key management. It has been developed by SAE Committee TEVEES18F, Vehicle Security Credentials Interoperability (VSCI), a subcommittee of SAE Committee TEVEES18A, Vehicle Cybersecurity Systems Engineering Committee. This committee is authorized under the scope and authority of the SAE Electronic Design Automation Steering Committee (also known as the Electronic Systems Group) that is directly under the scope and authority of the SAE Motor Vehicle Council.

The SAE Motor Vehicle Council's stated scope of influence and authority, as defined by the SAE includes, passenger car and light truck in conjunction with ISO/SAE 21434.

1.2 Safety versus Security

This document specifically pertains to the notion of cybersecurity; that is, in ensuring the resiliency of the system to, potentially malicious, external influences. However, in the construction of an automotive system, it is clear that safety also needs to be considered (that is, the cyber resiliency of the system to continually meet its expected correctness requirements).

While a security issue MAY have an impact on safety (e.g., the ability to make a given system infringe on its safety requirements), achieving an overall goal of both safety and security SHOULD not be mutually exclusive.

The adoption of a cybersecurity process adhering to techniques presented in this document neither allows for the system to meet its safety requirements nor precludes it. No method in this document either gives safety guarantees or limits the adoption of other techniques/standards that do.

1.3 Development Considerations

This document does not present, list, or document any techniques that fall outside of the scope of cybersecurity. To that end, it is expected that the adopter of this document will adhere to the recommended developmental considerations for the system that they are constructing. This includes the hardware, software, and system levels.

For example, this document does not outwardly cover topics such as programming language and real-time operating system selection, coding standards nor requirements driven testing.

These are all developmental considerations that MUST be addressed as part of the wider system development plan. Choices in the wider plan MAY have impact on the techniques that are required in this document.

This document does not define the relationships between the entities. These relationships are defined by the implementer(s).

It is expected that, prior to adopting this guideline, the correct level of rigor has been used to ensure that the system under consideration is being developed in the most appropriate way.

1.4 Purpose

The VSCI committee has come together to define a recommended practice around architecture, design, and key management protocol capabilities for automotive key management security via Key Management Interoperability Protocol (KMIP) utilization. This would include Key Management System (KMS) interfaces, in addition to the ecosystem constraints such as access control policies, key, and/or key attribute migration (using role-based separation which is modeled after Uptane, 2019), to avoid single points of failure in key generation and key storage systems.

1.5 How to Use This Document

This document SHOULD be used as a guideline when considering the management of and distribution of credentialing materials in the connected vehicle domain. Care SHOULD be given to open up dialogs between all parties that will either send, receive, or use the credentialing material to ensure that all understand the expectations and responsibility of each party in the exchange process.

1.6 Diagrams

Note that all diagrams in this document are sourced from the Automotive Key Management System (KMS) Annex A v0.9.2 dated August 2018, as developed by University of Michigan Transportation Research Institute (UMTRI). These diagrams may have changed since this writing.

2. REFERENCES

2.1 Applicable Documents

The following publications form a part of this specification to the extent specified herein. Unless otherwise indicated, the latest issue of SAE publications shall apply.

2.1.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or +1 724-776-4970 (outside USA), www.sae.org.

SAE J3101 Hardware Protected Security for Ground Vehicles

ISO/SAE 21434 Road Vehicles - Cybersecurity Engineering

2.2 Related Publications

The following publications are provided for information purposes only and are not a required part of this SAE Technical Report.

2.2.1 ISO Publications

Copies of these documents are available online at <https://webstore.ansi.org/>.

ISO/IEC/IEEE 1883:2016 Information Technology - Ubiquitous Green Community Control Network - Security

ISO 27000-1:2022 Information Security Management System

ISO 21789:2009 Gas Turbine Applications - Safety

2.2.2 NIST Publications

Available from NIST, 100 Bureau Drive, Stop 1070, Gaithersburg, MD 20899-1070, Tel: 301-975-6478, www.nist.gov.

FIPS 180-4 Secure Hash Standard (SHS)

FIPS 186-5 Digital Signature Standard (DSS)

SP 800-52 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations

SP 800-53 Security and Privacy Controls for Information Systems and Organizations

SP 800-56B Rev 2	Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography
SP 800-57 Part 1	Recommendation for Key Management: Part 1 - General
SP 800-57 Part 2	Recommendation for Key Management: Part 2 - Best Practices for Key Management Operations
SP 800-57 Part 3	Recommendation for Key Management: Part 3 - Application-Specific Key Management Guidance
SP 800-161	Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
SP 800-171	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

2.2.3 AUTOSAR Publications

Available from AUTOSAR, Niederfeldstrasse 18, 85413 Hörgertshausen, Germany, Tel: +49 87 64 78 93 99 40, <https://www.autosar.org/>.

AUTOSAR 948	Specification of Secure Hardware Extensions
-------------	---

2.2.4 IETF Publications

Available from the Internet Engineering Task Force (IETF), <https://www.rfc-editor.org/>.

RFC 4107	Guidelines for Cryptographic Key Management
----------	---

2.2.5 Other Publications

Cox, T. (2017). *Key management interoperability protocol (KMIP) version 1.4*. OASIS. Available at <https://docs.oasis-open.org/kmip/spec/v1.4/os/kmip-spec-v1.4-os.html>

Furlong, J. (2017). *Key management interoperability protocol useage guide version 1.4*. OASIS. Available at <http://docs.oasis-open.org/kmip/ug/v1.4/kmip-ug-v1.4.html>.

Hudson, T. and Joseph, M. (2017). *Key management interoperability protocol test cases version 1.4*. OASIS. Available at <http://docs.oasis-open.org/kmip/testcases/v1.4/kmip-testcases-v1.4.html>.

Hudson, T. and Lockhard, R. (2019). *Key management interoperability protocol profiles version 2.0*. OASIS. Available at <https://docs.oasis-open.org/kmip/kmip-profiles/v2.0/kmip-profiles-v2.0.html>.

ITUGSR, (2019). ITU-T X.509 (10/2019). Available at <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509>.

TCG. (2019). *Trusted platform module (TPM)*. Trusted Computing Group. Available at <https://trustedcomputinggroup.org/work-groups/trusted-platform-module/>.

Uptane. (2019). *IEEE-ISTO 6100.1.0.0 Uptane standard for design and implementation*. Uptane. Available at <https://uptane.github.io/papers/ieee-isto-6100.1.0.0.uptane-standard.html>.

3. DEFINITIONS AND ACRONYMS

For the purposes of this document, the following terms and definitions apply. ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO's online browsing platform: Available at <http://www.iso.org/obp>.
- IEC's Electropedia: Available at <http://www.electropedia.org/>.

These databases, along with the KMIP, were used in the creation of this section.

3.1 Definitions

3.1.1 ACCESS CONTROL

The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

(From ISO/IEC/IEEE 1883:2016.)

3.1.2 ACTIVE STATE

The key state in which a key MAY be used to cryptographically protect information (e.g., encrypt plain text or generate a digital signature), cryptographically process previously protected information (e.g., decrypt cyphertext or verify a digital signature), or both.

(From SP 800-53.)

3.1.3 ASSET

Something for which the compromise of its cybersecurity properties can lead to damage to a stakeholder.

3.1.4 ASYNCHRONOUS CORRELATION VALUE (ACV)

In the KMIP specification, asynchronous correlation value (ACV) is a byte string that is returned in the immediate response to an operation that is pending and that requires asynchronous polling.

(From OASIS. *Automotive Key Management System: Test Cases*, 2018.)

3.1.5 AUTHENTICATION

A process that provides assurance of the source and integrity of information in communications sessions, messages, documents, or stored data or that provides assurance of the identity of an entity interacting with the system.

(From SP 800-53.)

3.1.6 AUTHENTICATION CODE

A cryptographic check sum based on a security function.

(From Hudson and Joseph, 2017.)

3.1.7 AUTHORIZATION

Access privileges that are granted to an entity that convey an "official" sanction to perform a security function or activity.

(From SP 800-53.)

3.1.8 AVAILABILITY

Timely, reliable access to information by authorized entities.

(From SP 800-53.)

3.1.9 BACKUP

A copy of key information to facilitate recovery during the cryptoperiod of the key, if necessary.

(From SP 800-53.)

3.1.10 BATCH ITEM

The individual request or response within a batch.

(From Hudson and Joseph, 2017.)

3.1.11 CERTIFICATE

See definition for public key certificate ([3.1.83](#)).

3.1.12 CERTIFICATE AUTHORITY

The entity in public key infrastructure (PKI) that issues certificates to certificate subjects.

(Modified from SP 800-53.)

3.1.13 CERTIFICATE LENGTH

The length, in bytes, of an X.509 public key certificate.

(From Hudson and Joseph, 2017.)

3.1.14 CERTIFICATE SIGNING REQUEST (CSR)

In PKI systems, a certificate signing request is a message sent from an applicant to a registration authority of the PKI to apply for a digital identity certificate.

3.1.15 CIPHERTEXT

Data in its encrypted form.

(From SP 800-53.)

3.1.16 COMPROMISE

The unauthorized disclosure, modification, substitution, or use of sensitive key information (e.g., a secret key, private key, or secret metadata).

(From SP 800-53.)

3.1.17 COMPROMISED KEY STATE

A key state to which a key is transitioned when there is a suspicion or confirmation of the key's compromise.

(From SP 800-53.)

3.1.18 CONFIDENTIALITY

The property that sensitive information is not disclosed to unauthorized entities (e.g., the secrecy of the key information is maintained).

(From SP 800-53.)

3.1.19 CRYPTOGRAPHIC ALGORITHM

A well-defined computational procedure that takes variable input, including a cryptographic key resulting in an output.

(From SP 800-53.)

3.1.20 CRYPTOGRAPHIC KEY (KEY)

A parameter that is used in conjunction with a cryptographic algorithm that determines its operation in such a way that an entity with knowledge of the key can reproduce, reverse, or verify the operation while an entity without knowledge of the key cannot.

NOTE: Keys are owned and used by entities (humans, organizations, devices, or processes), that interact with other entities to conduct business. In the case of non-human owners, the owner is represented or sponsored by one or more humans.

EXAMPLE 1: A symmetric key used with Advanced Encryption Standard (AES) to encrypt plain text and decrypt cyphertext data.

EXAMPLE 2: A private signature key used with a digital signature algorithm to generate a digital signature.

EXAMPLE 3: A public signature verification key used with a digital signature algorithm to verify a digital signature

(Modified from SP 800-53.)

3.1.21 CRYPTO PERIOD

The time span during which a specific key is authorized for use or in which the keys for a given system or application MAY remain in effect.

(From SP 800-53.)

3.1.22 CUSTOMER

A person or organization that receives a service or product.

NOTE: In the context of this document, an organization is a business unit.

(From ISO/SAE 21434.)

3.1.23 DATA ENCRYPTION KEY

A key used to encrypt and/or decrypt data other than keys.

(Modified from SP 800-53.)

3.1.24 DEACTIVATED STATE

A key state in which the key(s) are not used to apply cryptographic protection (e.g., encrypt), but, in some cases, are used to process cryptographically protected information (e.g., decrypt).

(Modified from SP 800-53.)

3.1.25 DECRYPTION

The process of changing cyphertext into plaintext using a cryptographic algorithm and key.

(From SP 800-53.)

3.1.26 DESTROYED STATE

A key state to which a key is transitioned when it is destroyed. Although the key no longer exists, its previous existence MAY be recorded (e.g., in metadata or audit logs).

(From SP 800-53.)

3.1.27 DIGITAL SIGNATURE

The result of a cryptographic transformation of data that, when properly implemented with a supporting infrastructure and policy, provides the services of:

- Source/identity authentication.
- Data integrity and authentication.
- Support for signer non-repudiation.

(From SP 800-53.)

3.1.28 DOMAIN PARAMETER

A parameter used in conjunction with some public key algorithms to generate key pairs or to perform cryptographic operations (e.g., to create digital signatures or to establish key material).

(From SP 800-53.)

3.1.29 ENCRYPTED KEY

A cryptographic key that has been encrypted using an approved cryptographic algorithm to disguise the value of the underlying plaintext key.

NOTE: Approved cryptographic algorithms are algorithms that are agreed upon by the participants of the transaction.

(Modified from SP 800-53.)

3.1.30 ENCRYPTION

The process of changing plaintext into cyphertext using a cryptographic algorithm and key.

(From SP 800-53.)

3.1.31 ENTITY

An individual (human), organization, device, or process.

(Modified from SP 800-53.)

3.1.32 EPHEMERAL KEY

A cryptographic key that is generated for each execution of a cryptographic process (e.g., key establishment), and that meets other requirements of the key type such as being unique to each message or session.

(Modified from SP 800-53.)

3.1.33 GET FUNCTION

A function that returns the value of the variable name.

3.1.34 HASH FUNCTION

A function that maps a bit string of arbitrary (although bounded), length to a fixed length bit string. Approved hash functions satisfy the following properties:

- One way: It is computationally infeasible to find any input that maps to any pre-specified output.
- Collision resistant: It is computationally infeasible to find any two distinct inputs that map to the same output.

NOTE: Approved hash functions are functions that are agreed upon by the participants of the transaction.

(From SP 800-53.)

3.1.35 HASH VALUE

The result of applying a hash function to information. Also known as a digest.

(Modified from SP 800-53.)

3.1.36 INITIALIZATION VECTOR (IV)

A vector used in defining the starting point of a cryptographic process.

(From SP 800-53.)

3.1.37 INTEGRITY

A property whereby data has not been altered in an unauthorized manner since it was created, transmitted, or stored.

(From SP 800-53.)

3.1.38 INTEGRITY AUTHENTICATION

The process of obtaining assurance that the data has not been modified since an authentication code or digital signature was created for that data.

(From SP 800-53.)

3.1.39 INTEGRITY PROTECTION

The protection obtained for transmitted or stored data using an authentication code (e.g., message authentication code [MAC]), or digital signature computed on that data.

(From SP 800-53.)

3.1.40 KEY

See Cryptographic Key

3.1.41 KEY AGREEMENT

A key establishment procedure where keying material is generated from information contributed by two or more participants so that no party can predetermine the value of the keying material independently of any other party's contribution.

(From SP 800-53.)

3.1.42 KEY CONFIRMATION

A procedure used to provide assurance to one party that another party possesses the same keying material and/or shared secret.

(From SP 800-53.)

3.1.43 KEY DE-REGISTRATION

A function of the lifecycle of a cryptographic key; the marking of a key or the information associated with it (e.g., metadata), to indicate that the key is no longer in use.

(From SP 800-53.)

3.1.44 KEY DERIVATION

The process by which keying material is derived from either a pre-shared key or shared secret (based on the key agreement plan), along with other information.

(Modified from SP 800-53.)

3.1.45 KEY DESTRUCTION

To remove all traces of a cryptographic key so that it cannot be recovered by either physical or electronic means.

(From SP 800-53.)

3.1.46 KEY DISTRIBUTION

The transport of a key or other keying material from an entity that either owns, generates, or otherwise acquires the key, to another entity that is intended to use the key or key material.

(Modified from SP 800-53.)

3.1.47 KEY-ENCRYPTION KEY

A cryptographic key that is used for the encryption or decryption of other keys to provide confidentiality protection for those keys. Can also be known as a key-wrapping key.

(Modified from SP 800-53.)

3.1.48 KEY ESTABLISHMENT

A function in the lifecycle of a cryptographic key; the process by which cryptographic keys are securely established among entities using manual transport methods such as key loaders, automated methods such as key transport and/or key agreement protocols, or a combination of automated and manual methods.

(Modified from SP 800-53.)

3.1.49 KEY INFORMATION

Information about an individual key that includes all the key material associated with that key and associated metadata relating to that key.

(Modified from SP 800-53.)

3.1.50 KEY INVENTORY

Information about each key that does not include the key itself (e.g., the key owner, key type, algorithm, application, and expiry date).

(From SP 800-53.)

3.1.51 KEY (OR CERTIFICATE) INVENTORY MANAGEMENT

Establishing and maintaining records of keys and/or certificates in use, assigning and tracking their owners or sponsors, monitoring key and certificate status, and reporting the status to the appropriate official for remedial action when necessary.

(From SP 800-53.)

3.1.52 KEY LENGTH

The length of a key, in bits. Often used interchangeably with the term “key size.”

(Modified from SP 800-53.)

3.1.53 KEY MANAGEMENT

The activities involving the handling of cryptographic keys and other related key information during the entire lifecycle of the keys including their generation, storage, establishment, entry, output, use, and destruction.

(From SP 800-53, as well as Hudson and Joseph, 2017.)

3.1.54 KEY MANAGEMENT POLICY

A high-level statement of organizational key management policies that identifies a high-level structure, responsibilities, governing standards, organizational dependencies and other relationships, and security policies.

(From SP 800-53.)

3.1.55 KEY MANAGEMENT INTEROPERABILITY PROTOCOL (KMIP)

The Key Management Interoperability Protocol (KMIP) is an extensible communication protocol that defines message formats for the manipulation of cryptographic keys on a key management Server.

3.1.56 KEY MANAGEMENT SYSTEM (KMS)

A key management system (KMS), also known as a cryptographic key management system (CKMS), is an integrated approach for generating, distributing, and managing cryptographic keys for devices and applications. They MAY cover all aspects of security—from the secure generation of keys, over the secure exchange of keys, up to secure key handling and storage on the Client. Thus, a KMS includes the backend functionality for key generation, distribution, and replacement, as well as the Client functionality for injecting keys, storing, and managing keys on devices

3.1.57 KEY MANAGEMENT PRACTICE STATEMENT

A document or set of documents that describes in detail the organizational structure, responsible roles, and organizational rules for the functions identified in the key management policy.

(From SP 800-53.)

3.1.58 KEY PAIR

A public key and its corresponding private key; a key pair is used with a public-key algorithm.

(From SP 800-53.)

3.1.59 KEY RECOVERY

A function in the lifecycle of a cryptographic key; mechanisms and processes that allow authorized entities to retrieve or reconstruct the key from backups or archives.

(From SP 800-53.)

3.1.60 KEY REGISTRATION

A function in the lifecycle of a cryptographic key; the process of officially recording the keying material by a registration authority.

(From SP 800-53.)

3.1.61 KEY REVOCATION

A possible function of the lifecycle of a cryptographic key; a process whereby a notice is made available to affected entities that the key SHOULD be removed from operational use prior to the end of the established cryptoperiod of that key.

(From SP 800-53.)

3.1.62 KEY STATE

The states through which a key transition between its generation and its destruction.

- Pre-activation state.
- Active state.
- Suspended state.

- Deactivated state.
- Compromised state.
- Destroyed state.

(From SP 800-53.)

3.1.63 KEY TRANSPORT

Key establishment procedure whereby one party (the sender), selects and encrypts (wraps), the key then distributes it to another party (the receiver).

When used in conjunction with a public-key (asymmetric), algorithm, the key is encrypted using the public key of the receiver and subsequently decrypted using the receiver's private key

When used in conjunction with symmetric algorithm, the key is encrypted with a key-encryption key (wrapping key), that is shared by the sending and receiving parties and decrypted with the same key.

(Modified from SP 800-53.)

3.1.64 KEY UPDATE

A function performed on a cryptographic key to compute a new key that is related to the old key and is used to replace that key.

(Modified from SP 800-53.)

3.1.65 KEY WRAPPING

A method of encrypting one key using another key to securely store it or transmit it over an untrusted channel.

(Modified from Hudson and Joseph, 2017.)

3.1.66 KEYING MATERIAL

The factors that are used during the execution of a cryptographic algorithm. These factors include cryptographic keys, initialization vectors (IV), or domain parameters.

(Modified from SP 800-53.)

3.1.67 MANUAL KEY TRANSPORT

A non-automated means of transporting cryptographic keys by physically moving a device or document containing the key or share key.

(From SP 800-53.)

3.1.68 MASTER KEY

A key used with a key derivation method to derive additional keys. Can also be known as a key-derivation key.

(Modified from SP 800-53.)

3.1.69 MESSAGE AUTHENTICATION CODE (MAC)

A cryptographic check sum on data that uses an approved security function and a symmetric key to detect either accidental or intentional modifications of data.

NOTE: Approved security functions are functions that are agreed upon by the participants of the transaction.

(Modified from SP 800-53.)

3.1.70 METADATA

The information associated with a key that describes its specific characteristics, constraints, acceptable uses, ownership, etc. Portions of the metadata MAY be secret (e.g., the identity of the key's owner in some cases).

(From SP 800-53.)

3.1.71 NON-REPUDIATION

A service using a digital signature that is used to support a determination by a third-party of whether a message was signed by a given entity.

(Modified from SP 800-53.)

3.1.72 OPERATIONAL PHASE

A phase of the lifecycle of a cryptographic key whereby the key is used for standard cryptographic purposes.

(From SP 800-53.)

3.1.73 ORIGINAL EQUIPMENT MANUFACTURER (OEM)

A person or company having design responsibility for the equipment or for parts of it.

NOTE 1: This MAY be the manufacturer/packager of the equipment.

NOTE 2: This definition pertains to automotive vehicles and components.

(From ISO 21789:2009, ISO/IEC/IEEE 18883, SP 800-52)

3.1.74 OWNER

Certificate: A human entity that is identified as the subject in a public key certificate or is a sponsor of a non-human entity (e.g., device, application, or process), that is identified as the certificate subject.

3.1.75 KEY OR KEY-PAIR:

- Static key-pair: The entity that is associated with the public key and authorized to use the private key.
- Ephemeral key-pair: The owner is the entity that generated public/private key-pair.
- Symmetric key: The owner is the entity that is authorized to use the key.

(Modified from SP 800-53.)