Daimler Truck IT Security

Version 1.6

Basic security for DCS-T Certificates

Global Cyber Security

Table of contents

1. Table of revisions

Version	Datum	Editor	Changes
1.0	24.08.2018	C. Bader	Initial release.
1.1	26.09.2018	C. Bader	- Removed reference to DISF. - Reference to ISO 270XX added.
1.2	28.09.2018	C. Bader	Revision of section “introduction”.
1.3	24.03.2020	M. Wittiger	Adaption of the certificate owner to Mercedes Benz
1.4	31.08.2020	V. Hartmann	Initial Release for Daimler Truck AG Release
1.5	09.09.2020	V. Hartmann	Adaption of the certificate owner to Daimler Truck
1.6	01.09.2023	D. Gül	Adaptation of the content to Daimler Truck

2. Introduction

If not explicitly stated otherwise DCS-T certificates and the respective private keys are classified as follows:

	Confidentiality	Integrity	Availability
DCS-T certificate	Daimler Truck-internal	Daimler Truck-standard	Daimler Truck-standard
Private key to DCS-T certificate	Daimler Truck-confidential	Daimler Truck-standard	Daimler Truck-standard

To protect DCS-T certificates and the respective private keys organizational, procedural and technical controls shall be implemented according to the international information security standard ISO 27001 or a comparable acknowledged standard (e.g., TISAX) and using "state-of-the art" technology.

This document summarizes objectives and key controls to protect certificates and keys.

3. Objectives

DCS-T certificates and keys provided by Daimler Truck shall be protected according to state of the art. The following objectives and principles shall be applied:

Category	Objective
Information Security Organization	An ISMS is implemented and effectively operating. Roles and responsibilities with respect to information security are defined and communicated.
Asset management	Assets associated with DCS-T certificates and private keys and facilities processing them are identified and responsibilities are be assigned in order to protect them.
Access Control	Access to DCS-T certificates and private keys and facilities processing them will be controlled on the basis of business and security requirements and will generally only be granted on a need- to-know basis. Unauthorized access will be prevented through appropriate controls.
Cryptography	Cryptographic controls will be used properly and effectively to protect the confidentiality, authenticity and integrity of information.
Operations Security	Correct and secure operation of DCS-T certificate and private key processing facilities will ensure protection of software integrity and assurance of information confidentiality and integrity in electronic communications.
System Acquisition, Development and Maintenance	It is ensured that information security is an integral part of information systems across their entire lifecycle.
Information Security Incident Management	A consistent and effective approach for the management of information security incidents, including communication on security events and weaknesses will be established.

4. Key controls

In the sequel a relevant system (application, process) is defined as “a system (application, process) that stores or processes DCS-T certificates or respective keys or is related to processing DCS-T certificates or respective keys”.

The following key controls shall be implemented:

ID	Requirement
1	The contractor shall name a contact person for security management, which is responsible for all topics related to information security (security manager). He or she shall have sufficient authority and resources to investigate security incidents and remedy any arising information security issues.
2	The design of a relevant system (application, process) shall ensure confidentiality of DCS-T keys and authenticity and integrity of operations on that keys and answers according to state of the art.
3	Each project designing and implementing relevant systems, applications or processes not provided by Daimler Truck shall appoint a qualified security expert that is responsible for identifying and assessing security threats and risks and making them transparent to the application / process owner and the security manager who will report issues to Daimler Truck (cf. ID#5). Daimler Truck may ask for a proof of qualification of these technical expert.
4	Relevant systems and applications that are not provided by Daimler Truck shall be subject to security audit, source code analysis and penetration testing on a regular basis. The results shall be documented and reported to the security manager who will report issues to Daimler Truck (cf. ID#5).
5	The results from ID#3 and ID#4 shall be documented. a. Identified vulnerabilities and weaknesses shall be classified according to their criticality and remediated in time considering their criticality. b. b. Identified vulnerabilities and weaknesses shall be reported to the security manager who will report them to Daimler Truck.
6	Daimler Truck may ask for proof that security controls have been implemented and their effectiveness is being observed (right to audit).
7	Security-relevant events with respect to DCS-T certificates or respective keys shall be defined, logged and being monitored and reported to the appointed security manager (cf. ID#1) who will report to its Daimler Truck counterpart frequently.
8	Permission to request and access to *personal* DCS-T certificates or respective keys shall be granted only to centrally managed user accounts.
9	Entities shall be identified according to „Identity Proofing Objectives and Requirements v1.0“ before they are allowed to request personal DCS-T certificates or respective keys.
10	Access to keys for personal DCS-T certificates shall require 2 means of authentication.
11	It shall be transparent to the contractor which user has access to *non-personal* DCS-T certificates or respective keys. Upon request by Daimler Truck the contractor shall provide this information to Daimler Truck.
12	a. Cryptographic keys shall be protected according to state of the art while in transit and at rest. b. Passwords that protect DCS-T certificates or respective keys shall be configured according to state of the art.
13	Idle timeouts shall be configured after which re-authentication is required according to state of the art.
14	Applications handling and storing DCS-T certificates and keys shall be hardened and patched according to state of the art.

ID	Requirement
15	Systems handling and storing DCS-T certificates and keys shall be hardened and patched according to best practice.
16	Systems handling and storing DCS-T certificates shall have an Antivirus software running that is up to date and configured according to best practices.
17	All employees with access to DCS-T certificates or respective keys shall receive appropriate instruction in IT security awareness. a. Regular refreshers or updates shall take place. b. This shall be documented for each employee.
18	All employees with access to DCS-T certificates or respective keys shall sign a declaration of confidentiality.
19	If any of the above requirements cannot be met a formal risk analysis shall be carried out to assess the respective risk and ensure the risk is treated appropriately. The risk analysis shall be documented. The principal reserves the right to asses these analyses.

Requirements 13 – 15 are met on the diagnostic testing device if ZenZefiT is used for certificate management on the respective device.