MBUSA SCAN TOOL DATA LICENSE AGREEMENT

This MBUSA Scan Tool Data License Agreement (the "**Agreement**") is entered into as of XX-XX-XXXX (the "**Effective Date**"), by and between (INSERT) ("Licensee"), and Mercedes-Benz USA, LLC, a Delaware limited liability company with its principal office located at One Mercedes-Benz Drive, Sandy Springs, GA 30028 ("MBUSA"). Licensee and MBUSA are each referred to herein as a "Party" and, together, the "Parties".

RECITALS

WHEREAS, MBUSA has MBUSA Scan Tool Data (defined below), which provides uses for vehicle diagnostic scan tools;

WHEREAS, pursuant to a Data Services Agreement with the Equipment and Tool Institute ("ETI"), MBUSA has authorized ETI to facilitate access to the MBUSA Scan Tool Data to members of ETI who have entered into this Agreement with MBUSA; and

WHEREAS, Licensee desires to obtain Licensed Data (defined below) for use by Licensee as permitted herein.

NOW, THEREFORE, in consideration of the mutual promises and covenants contained in this Agreement, the parties agree as follows:

1. **Definitions**.

(a) "**Applicable Law**" means all applicable federal, state and local codes, orders, decrees, laws, statutes, ordinances, guidelines, rules, and regulations of any jurisdiction, including, without limitation, those of the U.S. Environmental Protection Agency ("EPA") and the California Air Resource Board ("CARB") pertaining to the dissemination of emission-related service information, as applicable to the subject matter of this Agreement, and the U.S. Export Administration Laws and Regulations ("EAR").

(b) "**ETI Agreement**" means the Data Services Agreement between ETI and MBUSA.

(c) "**Licensed Data**" means the MBUSA Scan Tool Data that is provided to Licensee, such as by ETI pursuant to the ETI Agreement.

(d) "**MBUSA Scan Tool Data**" means electronic messages transmitted between a scan tool and an electronic control unit ("ECU") on-board a Mercedes-Benz vehicle for the purposes of performing diagnosis, tests and repairs of a Mercedes-Benz vehicle, and includes, without limitation: (a) read only, data stream information (e.g. sensor values, I/O switch states, etc.); (b) bi-directional control, data stream information (e.g., operation of actuators, initiation of self-checks, etc.); (c) special diagnostic test routine requirements (e.g. VIN initialization, cylinder balance test, etc.); (d) vehicle data communication requirements (e.g., vehicle connector terminal/pin out definitions, physical layer definitions, etc.); (e) ECU data communication requirements (e.g. diagnostic protocols, data link layer definitions, etc.); and (f) vehicle application information (e.g. ECU information charts, etc.).

2. **Licensed Data**.

Subject to the terms of this Agreement, during the Term (defined below), MBUSA grants to Licensee a non-exclusive, non-transferable, non-sublicensable revocable right and license to the Licensed Data for the development, manufacture and sale of vehicle diagnostic service tools solely for the purposes of performing diagnosis, tests and repairs of Mercedes-Benz vehicles (the "Purposes"). The Licensee expressly acknowledges and agrees that, as between the parties, MBUSA (or its third party licensors) exclusively retain all ownership rights, title in and interest to the Licensed Data. Licensee's exercise of its rights under this Agreement shall not cause such ownership to merge for the benefit of Licensee or deprive or impair MBUSA of its ownership in and to any Licensed Data. Licensee shall not at any time do any act that impairs MBUSA's intellectual property and other rights therein. Licensee shall not use the Licensed Data for any purpose other than the Purposes, as defined herein. Licensee further agrees to not disclose such Licensed Data to any third party, except as expressly authorized herein or in a separately executed agreement. In addition, Licensee agrees not to duplicate, compile or reverse engineer all or any portion of the Licensed Data or provide the same in any form to any third party. Licensed data is solely for use in the NAFTA market for the purpose of diagnosis as stated in the agreement. Use of the diagnostic data outside of the NAFTA market will result in the termination of the license agreement pending further investigation.

3. **Confidentiality**.

(a) **Obligation of Confidentiality**. The Parties may exchange Confidential Information under this Agreement during the Term. For purposes of this section, "Confidential Information" means information disclosed by a Party (the "Discloser") to the other (the "Recipient"), whether in oral, written, or other tangible form, that could reasonably be considered confidential or proprietary, including the terms and conditions of this Agreement; business plans; pricing data and information, including pricing formulas; projected activities and results of operations; names of customers, counterparties, and employees; means, methods and processes of manufacture and assembly; intellectual property rights; existing and proposed products; computer software; ideas and concepts; data, drawings, designs, plans, specifications, materials and documents; and, business records. Confidential Information will not include information that (A) is or becomes publicly known through no act or omission of the Recipient in breach of this Agreement; (B) was in Recipient's lawful possession prior to the disclosure, as demonstrated by written records; (C) is rightfully received by Recipient from a third party without an accompanying secrecy obligation or breach of any duty or agreement by which the third party is bound, and imposes no obligation of confidentiality upon Recipient; or (D) is shown, by clear and convincing evidence, to be independently developed by Recipient's employees without having any access to Confidential Information and without any reliance in any way upon Discloser's Confidential Information.

A Recipient will use Discloser's Confidential Information exclusively for the purposes of performing Recipient's obligations under this Agreement (the "Authorized Use"). Recipient will

(i) treat as confidential the Confidential Information and protect the Confidential Information in the same manner and at a minimum with the same degree of care that Recipient protects its own trade secrets and other confidential business information; (ii) not alter, modify, disassemble, reverse engineer or decompile any of the Confidential Information; (iii) not, directly or indirectly, disclose, report or transfer Confidential Information to any third party without Discloser's prior written consent, except as explicitly provided herein; (iv) not, directly or indirectly, disclose, report or transfer Confidential Information to employees, directors or agents of Recipient or its affiliates, except for those employees, directors or agents who must have the information in order to accomplish the Authorized Use and who owe a duty or contractual obligation of confidentiality to Recipient; and (v) not use Confidential Information in any manner or form which will be in competition with Discloser or its business.

(b) **Permitted Disclosure**. If Recipient is requested or required (by oral questions, interrogatories, requests for information or documents in legal proceedings, subpoena, civil investigative demand or other similar process) to disclose Confidential Information, Recipient will provide Discloser with prompt written notice thereof so that Discloser may seek a protective order or other appropriate remedy and/or waive compliance with the provisions of this Agreement. If, in the absence of a protective order or other remedy or the receipt of a waiver, Recipient is nonetheless legally compelled to disclose Confidential Information to any tribunal or else stand liable for contempt or suffer other censure or penalty, Recipient may, without liability hereunder, disclose to such tribunal only that portion of the Confidential Information which Recipient is legally required to be disclosed, *provided* that Recipient exercises its best efforts to preserve the confidentiality of the Confidential Information (including by cooperating with Discloser, at Discloser's expense, to obtain an appropriate protective order or other reliable assurance that confidential treatment will be accorded the Confidential Information by such tribunal).

4. **Data Security**.

Licensee represents and warrants that it will comply with Exhibit B of this Agreement ("Data Protection Addendum") to protect the Licensed Data and any Confidential Information from unauthorized access or disclosure.

5. **Representations & Warranties**.

Each Party represents and warrants to the other Party that:

(1) it is duly organized, validly existing and in good standing as a corporation or other entity as represented in this Agreement under the laws and regulations of its jurisdiction of incorporation, organization or chartering;

(2) it will comply with all Applicable Laws in connection with their performance under this Agreement;

(3) it has the right, power and authority to enter into this Agreement, to grant the rights and licenses granted and to perform its obligations;

(4) the undersigned is authorization to execute this Agreement; and

(5) when executed and delivered, this Agreement will constitute the legal, valid and binding obligation of each Party, enforceable against each Party in accordance with its terms.

6. **Indemnity**.

(a) **Licensee Indemnification.** Licensee will defend, indemnify and hold harmless MBUSA and its affiliates and their respective officers, directors, employees, and agents (collectively, the "MBUSA Indemnitees"), from and against all third party actions, claims, suits, judgments, damages, liabilities, losses, penalties, costs and expenses (including attorneys' fees and disbursements) (collectively, "Losses") incurred or suffered by any MBUSA Indemnitee arising out of or relating to (i) any breach of this Agreement by Licensee; (ii) any actual infringement of a third-party's intellectual property rights including any patents, copyrights and copyrightable works (including computer programs), trade secrets or confidential information by Licensee; and (iii) any intentionally wrongful or grossly negligent acts or omissions by Licensee and its officers, directors, employees and agents, provided, that this clause (a) will not obligate Licensee to indemnify any MBUSA Indemnitee for any portion of damages (except for damages based on theories of strict liability) directly attributable to, and directly caused by, the negligence of an MBUSA Indemnitee.

(b) **MBUSA Indemnification**. MBUSA will defend, indemnify and hold harmless Licensee and its affiliates and their respective officers, directors, employees, and agents (collectively, the "Licensee Indemnitees"), from and against all third party Losses incurred or suffered by any Licensee Indemnitee arising out of or relating to (i) any breach of this Agreement by MBUSA; (ii) any actual infringement of a third-party's intellectual property rights including any patents, copyrights and copyrightable works (including computer programs), trade secrets or confidential information by MBUSA; and (iii) any intentionally wrongful or grossly negligent acts or omissions by MBUSA and its officers, directors, employees and agents, provided, that this clause (a) will not obligate MBUSA to indemnify any Licensee Indemnitee for any portion of damages (except for damages based on theories of strict liability) directly attributable to, and directly caused by, the negligence of an Licensee Indemnitee.

7. **License Fee and Insurance**.

(a) **License Fees**. Licensee will pay MBUSA an annual license fee as set forth on Exhibit A of this Agreement ("License Fee"). No Licensed Data will be provided to Licensee until Licensee has paid the License Fee. As set forth in the ETI Agreement, the License Fee shall be invoiced and collected by ETI, and ETI will subsequently remit the License Fee to MBUSA.

(b) **Insurance/Bonds**. Licensee agrees to provide and maintain, and shall require any agent or subcontractor it retains to provide and maintain, during the term of this Agreement and any extensions thereof, insurance coverage with companies acceptable to MBUSA as follows:

(1) Comprehensive general liability insurance covering bodily injury, property damage, personal and advertising injury, independent contractors and contractual liability, host liquor liability, products and completed operations liability for $1,000,000 each occurrence.

(2) Business automobile liability insurance covering all owned, hired and non-owned vehicles for a combined single limit bodily injury and property damage for $2,000,000 each occurrence.

(3) Workers' compensation insurance according to statutory limits, including employers' liability Insurance for $1,000,000 each accident, each disease, each employee, including within the policy a waiver of subrogation in favor of MBUSA.

(4) Umbrella Liability/Excess Liability providing coverage in excess of the Limits noted in subsections (1), (2) & (3) above at minimum Limits of Liability of $2,000,000. The Umbrella/Excess Policy must follow form of the Primary Policies noted in subsections (1), (2) & (3) above and be extended to "drop down" to become primary in the event the primary limits are reduced, or the aggregate limits are exhausted.

(c) Licensee will add MBUSA as an additional insured on the commercial general liability and business automobile liability and umbrella/excess liability policies stated herein. Licensee agrees and understands that this insurance will be primary over any other insurance that MBUSA maintains as respects to this Agreement. Licensee will include waiver of subrogation clauses in favor of MBUSA in all policies noted above including workers' compensation insurance.

(d) Licensee will furnish MBUSA certificates of insurance, upon execution of this Agreement evidencing the required coverages stated herein. Such certificates of insurance will provide for thirty (30) days advance written notice of cancellation, material change in coverage or non-renewal of coverage.

8. **Limitation of Liability**.

IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER (OR ANY OTHER PERSON OR ENTITY) FOR ANY SPECIAL, INDIRECT, EXEMPLARY, PUNITIVE, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, DAMAGES RESULTING FROM LOSS OF PROFITS OR LOSS OF BUSINESS) ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT, EVEN IF IT HAS BEEN ADVISED OF THEIR POSSIBLE EXISTENCE.

BOTH PARTIES FURTHER AGREE THAT IN NO EVENT SHALL ETI BE LIABLE TO EITHER OF THEM FOR ANY LIABILITY OR LOSSES OF ANY TYPE SUFFERED IN

CONNECTION WITH ANY ACTS OR OMISSIONS BY THE PARTIES RELATED TO THIS AGREEMENT.

9. **Term and Termination**.

(a) **Term**. Subject to clause (b) below, this Agreement will commence on the date hereof and will continue until the third anniversary of the date hereof (the "Initial Term"). The Initial Term will automatically renew for successive three-year periods (each, a "Renewal Term" and together with the Initial Term, each a "Term") unless a written notice of non-renewal is given by either Party at least 90 days prior to the end of the then-applicable Term.

(b) **Termination**. Each Party will have the right to terminate this Agreement, effectively immediately upon written notice, if the other Party fails to cure a material breach or default in the performance of its obligations under this Agreement within 14 days after receipt of written notice of such material breach or default from the non-defaulting Party.

10. **Force Majeure**.

Neither Party shall be responsible or liable for losses arising out of the delay or interruption of its performance of obligations under the Agreement due to any act of God, act of public enemy, act of governmental authority or due to riot, war, flood, terrorism, civil commotion, insurrection, severe weather conditions or any other cause beyond the reasonable control of the delayed Party.

11. Entire Agreement.

This Agreement, together with all Exhibits (or other attachments to this Agreement), and any other documents incorporated by reference to this Agreement, constitute the entire agreement between the Parties.

12. Assignment.

Neither Party may assign, transfer or delegate any or all of its rights or obligations under this Agreement without the prior written consent of the other Party. An assignment will not relieve the assigning Party of any of its obligations.

13. Headings.

Headings are inserted in this Agreement for reference purposes only, and may not be used to interpret this Agreement.

14. Severability.

If any term or provision of this Agreement is invalid, illegal or unenforceable in any jurisdiction, such invalidity, illegality or unenforceability shall not affect any other term or provision of this Agreement or invalidate or render unenforceable such term or provision in any other jurisdiction.

15. Governing Law; Jurisdiction.

This Agreement will be governed by and construed in accordance with the laws of the State of Georgia without giving effect to any choice or conflict of law provision or rule that would cause the application of laws of any jurisdiction other than those of the State of Georgia. Venue will be in the state or federal courts of Fulton County, Georgia.

16. Counterparts.

This Agreement may be executed in counterparts, each of which will be considered an original, but together will be considered one and the same agreement. A signed copy of this Agreement delivered by e-mail will be considered to have the same legal effect as delivery of an original signed copy of this Agreement.

17. **Marks**.

Neither Party may use the other Party's name, trade name, trademark, service mark, logo(s), or other identifying information or image, for any purpose unless specifically authorized in this Agreement or in writing by the other Party. In the event MBUSA authorizes such use under this Agreement or otherwise, such use shall be revocable at any time by MBUSA at MBUSA's sole discretion. The parties agree to adhere to the logo and trademark usage guidelines of the other Party when using that Party's name, logo(s), or other identifying information or image.

18. **Notice**.

All notices required to be given pursuant to this Agreement shall be in writing and shall be deemed effective: (i) when received in the event of service by certified mail, return receipt requested; (ii) when received by the Party at the address shown in this Agreement in the event of an overnight courier; or (iii) when sent via facsimile transmission (with a written copy sent simultaneously by United States mail). Any facsimile transmittal of any document related to this Agreement shall be treated in all manner and respects as the original document.

IN WITNESS WHEREOF, the parties have entered into this Agreement by having it signed by their duly authorized representatives.

____
(Licensee's Name)

____
____
____
(Licensee's Address)

By: __________________________________
(Signature)

____
(Printed Name)
Title:_____________________________ Date:
____

Mercedes-Benz USA, LLC

By:____________________________________
(Signature)

____
(Printed Name)
Title:___________________________

Date:___________________________

Exhibit A

License Fees

The amount stated in the schedule below, annually, is to be paid in advance to ETI on behalf of MBUSA pursuant to Section 7 of the Agreement. MBUSA reserves the right to change the fees set forth in the below schedule prior to any renewal of this Agreement. Licensee acknowledges and agrees that the below schedule that determines a lump sum annual License Fee based on Licensee's annual sales is a reasonable and expeditious way of approximating royalties in lieu of a per unit royalty.

	Annual Sales of Automotive Equipment and Tools in North America	Annual License Fee
	Under $10,000,000	$12,500
	$10,000,000 to $49,999,999	$14,500
	$50,000,000 and over	$17,500

<u>**Exhibit B**</u>

Data Protection Addendum

This Data Protection Addendum (the "Addendum") supplements the MBUSA Scan Tool Data License Agreement (the "Agreement") by and between Mercedes-Benz USA, LLC ("MBUSA") and the Licensee (as such term is defined in the Agreement, "Licensee") to which this Addendum is attached and/or incorporated by reference. All capitalized terms used in this Addendum shall have the meanings ascribed to them herein or, if not so ascribed herein, the meanings ascribed to them in the Agreement.

1. <u>Definitions.</u>

1.1 **MBUSA Data** means all data provided to or hosted by Licensee or which Licensee otherwise has access to while performing the Services, and which may include, without limitation, individual records or compilations thereof that include any or all of the following: (a) any commercially sensitive information about MBUSA, including, without limitation, information regarding mergers, acquisitions, consumer marketing preference data, lead generation source or other related sales data, or MBUSA employee compensation information; (b) MBUSA PII; and (c) information regarding MBUSA's information security program or infrastructure, including, without limitation, MBUSA Systems.

1.2 **MBUSA PII** means any MBUSA Data that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household. MBUSA PII includes, without limitation, data regulated as personal information or personal data by Privacy and Security Laws.

1.3 **MBUSA Systems** means any computer, computer network, computer application, imaging device, storage device, mobile computing device, or software that is owned, licensed, or leased by MBUSA or operated by a third party on behalf of MBUSA, which: (a) connects to or otherwise interacts with Licensee systems; or (b) is enabled or intended to access or interact with MBUSA Data created or Processed in connection with the Agreement.

1.4 **Privacy and Security Laws** means any and all international, local, country-specific, or U.S. State or Federal laws, regulations, directives, standards, guidelines, policies, or procedures, as amended, applicable to Licensee pertaining to the security, confidentiality, or privacy of MBUSA Data.

1.5 **Process** means to perform any operation or set of operations on MBUSA Data, including, without limitation, to: (a) collect, receive, input, upload, download, record, reproduce, store, host, organize, combine, log, catalog, cross-reference, manage, maintain, copy, adapt, alter, translate, or make other improvements or derivative works; (b) analyze, output, consult, use, disseminate, transmit, submit, post, transfer, disclose, or otherwise provide or make available; or (c) block, erase, delete, or destroy.

1.6 **Security** means technological, physical, organizational, and procedural safeguards, including, without limitation, policies, procedures, guidelines, practices standards, controls, hardware, software, firmware, and physical security measures, the function or purpose of which is, in whole or part, to protect the confidentiality, integrity, or availability of MBUSA Data.

1.7 **Security Breach** means any actual or reasonably suspected: (a) inability to access MBUSA Data due to an attack or exploit; (b) unauthorized or accidental access, acquisition, alteration, disclosure, use, theft, destruction, or loss to or of MBUSA Data; or (c) introduction of unauthorized code into MBUSA Systems.

1.8 **Secure Development Practices** refers to the utilization of methods or processes to ensure that software is free of vulnerabilities at anytime during the software life cycle. Secure Development Practices include, without limitation, observance of the OWASP framework and SANS Top 25 guidelines.

1.9 **Security Framework** refers to the ISO 27001 family of standards for Information Security Management Systems, the NIST Framework for improving Critical Infrastructure Cybersecurity, the Cloud Security Alliance Security Guidance, or other security framework approved in writing by MBUSA.

1.10 **Security Incident** means the successful or attempted exploitation of an existing vulnerability resulting in negative impact on the confidentiality, integrity, or availability of MBUSA Data, MBUSA Systems, or Licensee systems involved in the Processing of MBUSA Data.

1.11 **Services** means the service(s) that Licensee provides to MBUSA under the terms of the Agreement or any applicable SOW thereunder.

2. Data Processing.

2.1 Licensee shall only Process MBUSA Data to the extent necessary to provide the Services to MBUSA or as otherwise expressly permitted in the Agreement, the applicable SOW, or other written instructions from MBUSA, and for no other purpose.

2.2 Except as explicitly provided in the Agreement, Licensee shall make best efforts to provide MBUSA with unfettered, uninterrupted, and constant access to MBUSA Data, and shall make best efforts to delete, correct, or block any such data, or allow MBUSA to do the same, upon MBUSA’s written request.

2.3 Upon request, Licensee shall provide to the MBUSA Information Security contact a list of each and every physical location at which either Licensee or and each of Licensee’s subcontractor(s) will Process MBUSA Data.

2.4 Licensee shall make reasonable efforts to assist MBUSA as needed to respond to requests from authorities, data subjects, customers, or others to provide information (including details of the Services provided by Licensee) related to Licensee’s Processing of MBUSA Data.

3. Information Security; Compliance.

3.1 Licensee is responsible for the Security of any MBUSA Data to the extent it Processes such data. Licensee shall, at its sole cost and expense, implement Security that is no less rigorous than, and shall only Process MBUSA Data in such a manner so as to comply with: (a) the Security Framework; (b) Privacy and Security Laws; and (c) any other requirements of this Addendum or the Agreement. Licensee shall immediately notify MBUSA if Licensee knows that any written instruction by MBUSA would cause either or both parties to violate Privacy and Security Laws.

3.2 At a minimum, Licensee’s Security shall include: (a) access controls; (b) physical security; (c) protection of MBUSA Data at rest and in transit; (d) segregation of MBUSA Data from other data; (e) privacy and security awareness training; (f) record maintenance, including, without limitation, incident and compliance recordkeeping consistent with the Security Framework; (g) Secure Development Practices with regard to applications that Process MBUSA Data; and (i) incident, vulnerability, and vendor management programs.

3.3 Remote access to MBUSA Data or MBUSA Systems is only allowed upon prior written approval by MBUSA, and must occur through access points approved by MBUSA. Licensee systems used for such remote access must be protected according to the requirements of this Addendum.

3.4 [Intentionally omitted].

3.5 Licensee shall ensure only Licensee-owned or leased devices are used by Licensee and its subcontractors to Process MBUSA Data and shall promptly notify MBUSA of any lost or stolen device that was used to Process MBUSA Data.

3.6 Licensee shall obtain MBUSA's prior written consent before implementing any change to the Processing of MBUSA Data that constitutes a material change in Licensee's Security. Licensee shall use commercially reasonable efforts to provide MBUSA at least ninety (90) days' notice in advance of the proposed effective date of such change. To the extent Licensee implements any such change without MBUSA's written consent, MBUSA shall have the right to terminate the Agreement, the applicable SOW, or this Addendum effective immediately upon written notice to Licensee.

3.7 Licensee shall assign a knowledgeable employee working for Licensee that shall act as its Security Coordinator, who will be the security liaison between MBUSA and Licensee.

3.8 During the term of the Agreement, Licensee shall implement and maintain additional Security, as mutually agreed upon by Licensee and MBUSA, in the event of: (a) any material changes to Services; (b) any Security Breach or Security Incident; or (c) any material decreases to Licensee's Security; provided, that the failure of MBUSA to make a request of Licensee shall not impact, eliminate, or decrease Licensee's obligations under this Addendum.

3.9 Licensee shall cooperate with MBUSA's reasonable requests to assist MBUSA with its own compliance objectives pursuant to Privacy and Security Laws, including, without limitation, completing any documentation, assessments, or questionnaires provided to Licensee regarding the same with complete and accurate information and complying with any data subjects' requests to block, correct, or delete their data from Licensee's systems.

3.10 Licensee shall, to the extent permitted by law, notify MBUSA immediately upon receipt of any request from a regulator to access MBUSA Data, including any request to access locations where such information is stored.

3.11 In the event of any conflict among any of Licensee's obligations as required herein or as required in the Agreement, Licensee shall comply with the obligation that provides the most protective Security.

4. <u>Security Breach Procedures.</u>

4.1 Licensee shall notify MBUSA as soon as practicable, and in any event within twenty-four (24) hours, after Licensee becomes aware of any Security Incident or Security Breach.

4.2 Licensee shall, at its sole cost and expense, use best efforts to immediately remedy any

Security Incident or Security Breach and use best efforts to prevent any further Security Incident or Security Breach.

4.3 Licensee shall, at its sole cost and expense: (a) promptly preserve all relevant records, logs, files, data reporting, and other materials relevant to any Security Incident or Security Breach, and shall provide the same to MBUSA upon request; and (b) diligently investigate any Security Incident or Security Breach and shall fully cooperate with MBUSA in its own investigation of and response to any such Security Incident or Security Breach.

4.4 If a Security Incident or Security Breach arises, in whole or in part, from an act or omission of Licensee, Licensee shall reimburse MBUSA for all reasonable costs incurred by MBUSA in responding to, and mitigating damages caused by, any such Security Incident or Security Breach, including, without limitation, all costs of notice and credit monitoring and identity theft protection services.

4.5 Unless otherwise required by law, Licensee agrees that it shall not inform any third party of any Security Incident or Security Breach without first obtaining MBUSA's prior written consent, other than to inform a complainant that the matter has been forwarded to MBUSA's legal counsel. Further, Licensee agrees not to include MBUSA's name, logo, or any other identifiable information about MBUSA or its affiliates in any notice or public statement concerning any Security Incident or Security Breach without MBUSA's prior written approval.

5. <u>Confidentiality.</u>

Licensee shall hold any information or data communicated to or otherwise obtained by Licensee by virtue of Licensee's delivery of Services in confidence and adhere to industry best practices for securing such information or data.

6. <u>Subcontractors.</u>

6.1 Licensee shall only provide access to MBUSA Data or to Licensee's systems that would allow access to MBUSA Data to subcontractors to the extent necessary for Licensee to perform the Services for MBUSA. Once any such subcontractor no longer needs access to MBUSA Data in order for Licensee to perform Services for MBUSA, Licensee shall immediately terminate such subcontractor's access to such MBUSA Data, or, if applicable, shall immediately request that MBUSA terminate such access.

6.2 Prior to providing any subcontractor with access to MBUSA Data or to Licensee's systems or network that would allow access to MBUSA Data, Licensee shall: (a) conduct a reasonable investigation of such subcontractor's Security measures to determine that such Security is reasonable and consistent with Licensee's obligations under this Addendum; and (b) ensure that such subcontractor is obligated by law or contract to protect MBUSA Data in a way that is consistent with Licensee's obligations to protect MBUSA Data under this Addendum. Notwithstanding anything to the contrary herein, in all events, Licensee is and shall remain fully responsible for any act, error, or omission of any subcontractor to whom Licensee grants access to MBUSA Data or to Licensee's systems or network that would allow access to MBUSA Data with respect to compliance with this Addendum, as if such act, error, or omission was undertaken by Licensee.

6.3 Licensee shall provide to MBUSA at the outset of the Agreement a complete list of all subcontractors who will Process MBUSA Data in furtherance of Licensee's provision of Services to MBUSA, and shall update such list as necessary throughout the term of the Agreement; provided, however, that Licensee shall not engage any subcontractor to Process MBUSA Data except as explicitly set forth in this Section 6.

7. Monitoring & Audits.

7.1 Licensee agrees to allow MBUSA and its representatives to, and shall secure MBUSA and its representatives' rights to, monitor, log, and analyze access by Licensee and each of its subcontractors within MBUSA Systems as a condition of allowing such access.

7.2 Upon MBUSA's written request, Licensee must permit MBUSA or its representative to annually audit any and each of Licensee's privacy and security controls in relation to any MBUSA Data being Processed by Licensee. Licensee shall fully cooperate with such audit by providing access to knowledgeable personnel, physical premises, documentation, infrastructure, and application software relevant to Licensee's compliance with this Addendum. Licensee shall make available documentation from its subcontractors to support MBUSA's audit upon MBUSA's request.

7.3 Licensee shall, at its sole cost and expense, maintain sufficient and current external security assessments of controls relevant to the Processing of MBUSA Data to demonstrate Licensee's compliance with this Addendum ("Assessments") and provide a copy of such Assessments to MBUSA upon request. Sufficient Assessments include a SOC-2 Type 2 report, ISO 27001 certification, CSA Security Trust Assurance and Risk (STAR) Level 2 certification, or other external audit or report that may be agreed upon by MBUSA. Licensee will notify MBUSA immediately if Licensee fails an Assessment.

7.4 Following any audit by MBUSA or MBUSA's review of Licensee's most recent Assessment, Licensee shall, as soon as reasonably practicable and at its sole cost and expense, implement any measures requested in writing by MBUSA which are reasonably necessary for Licensee to meet its obligations under this Addendum.

8. Term and Termination.

8.1 This Addendum shall be effective as of the Effective Date of the Agreement, and shall remain in effect until the later of either: (a) the duration of the Agreement; or (b) for so long as Licensee or any of its subcontractors continues to Process MBUSA Data, provided that MBUSA may reasonably assume that Licensee's and its subcontractors' Processing activities are continuing until MBUSA receives written confirmation from Licensee to the contrary.

8.2 This Addendum may be terminated by MBUSA for any reason upon thirty (30) days' written notice to Licensee.

8.3 Promptly upon expiration or termination of the Agreement or anytime earlier upon MBUSA's prior written request, Licensee shall, at its sole cost and expense, permanently delete or migrate to MBUSA or any third-party vendor of MBUSA (the choice to be made by MBUSA in its sole discretion), and shall cause its subcontractors to do the same, any and all MBUSA Data in Licensee's or its subcontractors' possession or control, including, without limitation, from backup and archival sources, in compliance with industry standards, Privacy and Security Laws, and otherwise as specified in this Addendum. To the extent MBUSA Data is to be permanently deleted under this provision, Licensee will, upon MBUSA's request, provide written certification of the permanent deletion of such MBUSA Data. To the extent MBUSA Data is to be migrated to MBUSA or another third-party vendor under this provision, such MBUSA Data will be in a format specified by MBUSA or, if not specified, in a platform-agnostic format, and Licensee shall, at its sole cost and expense, reasonably cooperate with MBUSA and the recipient third-party vendor (if applicable) as necessary to carry out such migration.

8.4 A Security Breach arising, in whole or in part, from an act or omission of Licensee or breach of Licensee's obligations under this Addendum shall constitute an event of default under the Agreement entitling MBUSA to terminate the Agreement or the applicable SOW immediately and without opportunity to cure by providing written notice of such termination to Licensee. Without limitation to any other right or remedy set forth in this Addendum, the Agreement, or the applicable SOW, in the event that the Agreement or any SOW thereunder is terminated by Licensee pursuant to this Section 8.4, MBUSA shall be entitled to recover from Licensee the reasonable costs incurred by MBUSA in obtaining services from an alternate vendor to replace the terminated Services. Additionally, if MBUSA so elects in its sole discretion, Licensee shall, upon written notice from MBUSA, continue to provide the terminated Services in accordance with the Agreement and the applicable SOW until such time as MBUSA can obtain such replacement services from an alternate vendor, provided that: (a) Licensee shall be entitled to standard compensation as set forth in the applicable SOW for its performance of the terminated Services during such period; and (b) in no event shall Licensee have any obligation under this provision to provide the terminated Services past the date that the term of the applicable SOW would have otherwise expired.

9. Miscellaneous.

9.1 **Insurance Coverage**. In addition to any insurance requirements specified in the Agreement or any Exhibit thereto, Licensee shall also maintain Privacy and Network Security (otherwise known as Cyber Liability) coverage which includes providing protection against liability for: (a) system attacks; (b) denial or loss of service attacks; (c) spread of malicious software code; (d) unauthorized access and use of computer systems; (e) crisis management and customer notification expenses; (f) privacy regulatory defense and penalties; and (g) liability arising from the loss or disclosure of data that would encompass MBUSA Data; in each case, with coverage limits of not less than $5,000,000 per claim. Prior to commencing any performance under the Agreement, Licensee shall provide MBUSA with a certificate of insurance evidencing the insurance coverage required in this Section 9.1.

9.2 **Equitable Relief**. Licensee recognizes that serious and irreparable injury could result to MBUSA if Licensee breaches its obligations under this Addendum. Therefore, Licensee agrees that MBUSA will be entitled to a restraining order, injunction, or other equitable relief if Licensee breaches its obligations under this Addendum, in addition to any other remedies and damages that would be available at law or in equity.

9.3 **Indemnification**. Without limitation to any other indemnification obligation under the Agreement, Licensee shall defend, indemnify, and hold harmless MBUSA, its affiliates, and each of their respective employees, officers, directors, agents, and representatives from and against all liabilities, losses, damages, judgments, settlements, obligations, fines, costs, and expenses of any nature (including, without limitation, reasonable attorneys' fees and litigation costs) incurred in connection with any claim, action, cause of action, suit, demand, or proceeding threatened or asserted by any third party (including, without limitation, any government entity) arising out of, relating to, or resulting from (i) any Security Incident or Security Breach arising, in whole or in part, from an act or omission of Licensee or (ii) any failure by Licensee to comply with any of the requirements set forth in this Addendum.

9.4 **Liability**. MBUSA'S DAMAGES RESULTING FROM (i) ANY SECURITY INCIDENT OR SECURITY BREACH ARISING, IN WHOLE OR IN PART, FROM AN ACT OR OMISSION OF LICENSEE OR (ii) ANY FAILURE BY LICENSEE TO COMPLY WITH ANY OF THE OBLIGATIONS SET FORTH IN THIS ADDENDUM ARE NOT SUBJECT TO ANY LIMITATIONS OR EXCLUSIONS OF LIABILITY SET FORTH IN THE AGREEMENT. FURTHER, THE FOLLOWING REASONABLE COSTS SHALL BE CONSIDERED DIRECT DAMAGES IF SUSTAINED BY MBUSA ARISING OUT OF ANY SUCH SECURITY INCIDENT OR SECURITY BREACH OR ANY FAILURE BY LICENSEE TO COMPLY WITH ANY OF THE OBLIGATIONS SET FORTH IN THIS ADDENDUM: (a) COSTS ARISING FROM PROCURING SERVICES FROM AN ALTERNATIVE SOURCE; (b) COSTS ARISING FROM CREATING OR RELOADING LOST OR DAMAGED MBUSA DATA; (c) COSTS ARISING FROM MBUSA'S INVESTIGATION OR REMEDIATION OF SUCH SECURITY INCIDENT OR SECURITY BREACH OR FAILURE OF LICENSEE TO COMPLY WITH THE OBLIGATIONS SET FORTH IN THIS ADDENDUM, INCLUDING, WITHOUT LIMITATION, FORENSIC INVESTIGATION, PREPARATION AND DELIVERY OF NOTIFICATION, AND PROVISION OF CREDIT MONITORING AND IDENTITY THEFT PROTECTION SERVICES; AND (d) LEGAL FEES ASSOCIATED WITH EACH OF THE FOREGOING.

10. <u>State-Specific Provisions.</u>

10.1 **California Consumer Privacy Act Provisions**.

(a) <u>Scope</u>. The provisions of this Section 10.1 are included in this Addendum for the purpose of ensuring compliance with the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 *et seq.* (the "CCPA"). Except as modified in this Section 10.1, all other provisions of this Addendum shall remain in full force and effect.

(b) <u>Definitions</u>. For purposes of this Section 10.1 only, the following terms shall have the following meanings: (i) "MBUSA Personal Information" means any personal information that MBUSA discloses to Licensee for any business purpose pursuant to the Agreement; (ii) "personal information" has the meaning set forth in Cal. Civ. Code § 1798.140(o); (iii) "business purpose" has the meaning set forth in Cal. Civ. Code § 1798.140(d); (iv) "commercial purpose" has the meaning set forth in Cal. Civ. Code § 1798.140(f); (v) "sell" has the meaning set forth in Cal. Civ. Code § 1798.140(t); and (vi) "service" has the meaning set forth in Cal. Civ. Code § 1798.140(u).

(c) <u>Restrictions on MBUSA Personal Information</u>. Licensee is prohibited from: (i) selling any MBUSA Personal Information; (ii) retaining, using, or disclosing any MBUSA Personal Information for any purpose other than for the specific purpose of performing the Services, including retaining, using, or disclosing the MBUSA Personal Information for any commercial purpose other than providing the Services; and (iii) retaining, using, or disclosing any MBUSA Personal Information outside of the direct business relationship between MBUSA and Licensee.

(d) <u>Certification</u>. By signing the Agreement, Licensee certifies that it understands the restrictions in Section 10.1(c) and will comply with them.

Exhibit C

General Terms and Conditions (GTCs) for DCS Certificates (CeBAS) Addendum

This DCS Certificate (CeBAS) Addendum (the "Addendum") supplements the MBUSA Scan Tool Data License Agreement (the "Agreement") by and between Mercedes-Benz USA, LLC ("MBUSA") and the Licensee (as such term is defined in the Agreement, "Licensee") to which this Addendum is attached and/or incorporated by reference. All capitalized terms used in this Addendum shall have the meanings ascribed to them herein or, if not so ascribed herein, the meanings ascribed to them in the Agreement.

1. Scope and Agreement components.

1.1 The provision by MBUSA, or one of its affiliated companies, of digital certificates with respective associated private key to access control devices ("DCS Certificates") is exclusively subject to the following terms and conditions. Any general terms and conditions of the company intending to use DCS Certificates (the "User") are not part of the Agreement, even if these are included with calls for tenders, orders, or declarations of acceptance and no objection was raised to them.

1.2 To protect DCS 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 (eg., TISAX) and using "state-or-the art" technology.

2. Subject of the Agreement

2.1 This Agreement regards the provision of DCS Certificates for accessing control devices on a loan basis. DCS Certificates are needed for secure diagnosis, secure coding and secure onboard vehicle communications and are provided exclusively for this purpose.

2.2 By these GTCs the overall regulations for DCS certificates are agreed upon ("Framework Agreement"). Each certificate issued establishes a separate lending relationship ("Individual Contract") for the specific DCS Certificate under this Framework Agreement.

2.3 A DCS Certificate is either issued for a natural person ("DCS Certificate Holder") or for a User with an assigned person named by the User to be competent and responsible for ensuring its proper handling ("DCS Certificate Responsible").

3. Conclusion of the Agreement

3.1 These GTCs as the Framework Agreement must be established in writing and signed by or incorporated as an exhibit into an agreement signed by both parties.

3.2 Any offer made by the User to MBUSA regarding the conclusion of the Framework Agreement can exclusively be submitted in writing. MBUSA will provide offer acceptances in writing.

3.3 Each issue of a DCS Certificate establishes a separate lending relationship. The User shall ensure that only its authorized representatives request only such DCS Certificates for the respective DCS Certificate Holder or DCS Certificate Responsible that are needed to fulfill their tasks.

3.4 A lending relationship for a specific DCS Certificate is established when MBUSA explicitly accepts a request for this DCS Certificate in writing or issues the DCS Certificate.

3.5 A DCS certificate may only be requested for a User's group company under the following conditions: Prior to the request, the User ensures by way of a contract with the group company that any obligations towards MBUSA as well as any rights of MBUSA based on the Framework Agreement and any Individual Contract are agreed upon with direct effect for MBUSA and remain into effect for the term of any issued DCS Certificates. The group company is only entitled to request a DCS Certificate after prior provision of the respective contract by the User as appropriate proof of compliance with these conditions. The User shall guarantee compliance with these conditions and the obligations of a group company.

4. Contractual performance

4.1 The characteristics of each DCS Certificate are defined by the current Certificate Description from MBUSA at the time when each Individual Contract is concluded.

4.2 A DCS Certificate shall be provided in the manner offered by MBUSA at the time when each Individual Contract is concluded. This could involve sending a digital transmission using an encrypted PKCS#12 container, for instance, or making it available for DCS Certificate retrieval by software offered by Mercedes-Benz Group AG ("MBAG") for this purpose (such as ZenZefi).

4.3 In the event of any questions in connection with a DCS Certificate, the User can contact an information source designated by MBUSA.

5. Conditions for using DCS Certificates

5.1 A DCS Certificate is issued either to a DCS Certificate Holder or to a User with assignment of a DCS Certificate Responsible. The User shall ensure that the provisions of these GTCs are followed by the DCS Certificate Holder or DCS Certificate Responsible, on whose behalf it has requested DCS Certificates. Any violations by DCS Certificate Holders or DCS Certificate Responsibles or authorized persons (see section 5.5) shall always be attributed to the User. If a DCS Certificate Holder or DCS Certificate Responsible violates the provisions of these GTCs, MBUSA can prohibit the further use of the DCS Certificates in whole or in part. If a DCS Certificate is requested for one of the User's sub-contractors, these provisions shall apply accordingly. In this case, the User shall particularly ensure by way of a contract that the User's obligations based on the Framework Agreement and the respective Individual Contract have been passed on to the subcontractor beforehand.

5.2 The use of DCS Certificates is only permissible at the User's own sites, only within the scope of the intended purpose for the respective certificates, and only by the DCS Certificate Holder or under the supervision and responsibility of the respective DCS Certificate Responsible, with no private use permitted.

5.3 For the use of DCS Certificates only devices with access protection and security mechanisms that meet the current MBUSA requirements at the time when the certificate was issued are permissible. When using the DCS Certificates, the requirements of the norm ISO 27001 or acknowledged comparable norms (such as Automotive TISAX) and the MBUSA security requirements as per Annex 1 of these GTCs ("Basic Security for DCS Certificates") in accordance with the current state-of-the-art must be observed. In the event of any ambiguity, the User shall consult its contact partner at MBUSA for clarification.

5.4 Prerequisite for the handling of DCS Certificates is the use of software provided or explicitly approved by MBAG for this purpose (such as ZenZefi). The User must ensure that the security requirements are fulfilled, and shall demonstrate this by submitting a suitable security concept. Under no circumstances a DCS Certificate may be accessed by using software which was not provided or explicitly approved by MBAG (such as ZenZefi).

5.5 Using DCS Certificates requires strict compliance with the obligations and definitions in these GTCs, both by the User and by any persons authorized by the User to work with the DCS Certificates. In addition to the DCS Certificate Holder and the DCS Certificate Responsible, authorized persons also include such natural persons who are required as per these GTCs to work with DCS Certificates and to interact with the necessary software for the use of DCS Certificates ("need-to-know principle"). If these requirements are not fulfilled or are no longer completely fulfilled, MBUSA can prohibit the further use of DCS Certificates, in whole or in part, with immediate effect.

6. Security obligations of the contractual partner

6.1 The User shall ensure that the IT infrastructure used for handling the DCS Certificates, as well as access to the DCS Certificates, complies with MBUSA's current security requirements (see section 5.3). This also applies to connections through local networks and storage media.

6.2 MBUSA can make appropriate changes to the requirements named in section 6.1, and shall notify the User of any changes in a suitable manner. The changed version shall become binding two weeks after notification of the User. The User can only terminate the Framework Agreement as a whole, together with all of the Individual Contracts, within two weeks of receiving notice of a changed version, in writing, with immediate effect, if the User does not agree to the changes (special termination right).

6.3 At the latest when a DCS Certificate is requested, the User shall ensure that all security precautions are fulfilled.

7. Confidentiality obligations of the contractual partner

7.1 The DCS Certificates and any associated information, as well as the content of this Framework Agreement, are to be treated strictly confidential. Any use of the DCS Certificates, information, and agreement content beyond the agreed purpose of the specific DCS Certificate issued shall always constitute a serious violation of MBUSA's company and trade secrets. This does not apply to passing on contractual content to group companies (see section 3.5) or subcontractors (see section 5.1) as far as the User is obligated to pass on the contractual obligations of these GTCs to a group company or a subcontractor.

7.2 The User shall only entrust persons with access to DCS Certificates and with the use of the necessary software and systems, in which the DCS Certificates are used, who are required to use them according to these GTCs.

7.3 The User shall prevent any handling of the DCS Certificates by persons who are not entrusted with such handling according to these GTCs. This particularly applies to personnel who are not assigned to the specific order that requires access to DCS Certificates and are correspondingly obligated to maintain confidentiality.

7.4 Any possible access by third parties, who are not entrusted with the handling of DCS Certificates and the use of the necessary software for DCS Certificates, is strictly prohibited. Also strictly prohibited is any disclosure to third parties of the access information for systems and applications that a User is using for the handling of DCS Certificates.

7.5 In addition, the User's confidentiality obligations as agreed for the respective order placement shall apply as far as these requirements contain stricter or further extensive requirements than these GTCs.

8. Information and correction obligations

8.1 At MBUSA's request, the User shall provide unlimited, immediate and comprehensive information about all security and confidentiality measures relating to the handling of DCS Certificates, as well as compliance with and controlling of these. To this end, the User shall provide corresponding documentation and data along with explanations. Upon request, the User shall permit MBUSA to review these security and confidentiality measures or to have them reviewed by third parties who are obligated to maintain confidentiality. Upon request, the User shall provide MBUSA with the necessary audit reports as proof of appropriate security and confidentiality measures for subcontractors who have or could gain access to DCS Certificates.

8.2 The User shall immediately provide MBUSA with detailed information about any inadequate security or confidentiality measures and about any suspected violations of such measures, without being requested, first in text form and then in writing to the address designated by MBUSA and the User shall, upon request, immediately provide any additionally requested information in this regard without limitation. This also applies to any foreseeable access or access attempts by third parties to devices for the use of DCS Certificates.

8.3 The User shall immediately rectify any inadequacy of security or confidentiality measures and shall inform MBUSA of corresponding measures immediately, first in text form and then in writing to the address designated by MBUSA.

9. Other requirements

9.1 The User shall appoint a general contact person who is responsible for executing this Agreement, and shall provide this name to the address designated by MBUSA. MBUSA shall appoint a general contact person for this Agreement.

9.2 In case of doubt, the User shall provide proof of compliance with contractual obligations also by its appointed personnel and subcontractors.

9.3 It is the User's responsibility to ensure operations in the working environment for the DCS Certificate, particularly the systems for using DCS Certificates, and to provide adequate protection from outages.

9.4 The User shall immediately report any disruptions in the use of DCS Certificates to the address designated by MBUSA. This shall not establish any rights of the User.

9.5 MBUSA is entitled to monitor and audit the performance of measures to implement the obligations from these GTCs (and the additional provisions), particularly compliance with usage rights for DCS Certificates, either itself or through third parties who are obligated to confidentiality, on site as well. The User shall provide the necessary information and present corresponding documentation completely, as well as granting access to sites where the systems containing DCS Certificates are located, including the rooms and computer systems. The User shall bear the costs of an audit if a violation of the obligations from these GTCs is determined; otherwise, MBUSA shall bear the costs. Upon request, the User shall provide MBUSA with the necessary audit reports as proof of compliance with the obligations from these GTCs for any subcontractors who have or could gain access to DCS Certificates.

9.6 MBUSA can bindingly object to specific persons' use of DCS Certificates at any time for any not insignificant reason.

10. Compensation

10.1 MBUSA shall make the DSC Certificates available with the completion of MBUSA's Vendor License Agreement and payment associated with procurement of each MBUSA Diagnostic Data package.

11. Warranty

11.1 The DCS Certificates shall be provided as they are used by MBUSA. Warranty rights shall only exist if MBUSA is responsible for either intent or gross negligence, or if MBUSA has fraudulently concealed a defect. This also applies to any support services.

11.2 The User shall immediately report any defects in comprehensible, detailed form, including all information that is helpful for identifying and analyzing the defect, in writing or electronically to the address designated by MBUSA. In particular, this must include the work steps that led to the defect, the manner in which it appeared, and its effects. Unless otherwise agreed, the corresponding forms and procedures of MBUSA shall be used.

12. Liability

12.1 MBUSA shall provide damage compensation or compensation for futile expenditures, regardless of legal grounds (e.g. for legal transaction or similar obligations, a violation of obligations, or unlawful actions), without limitation in the event of intent or gross negligence; for the injury of life, body or health; and according to the provisions of the Product Liability Law. MBUSA shall not be held liable beyond this.

12.2 The above liability limitation shall also apply to the personal liability of MBUSA's employees, representatives, corporate bodies, and vicarious agents.

12.3 MBUSA reserves the right to claim contributory negligence.

12.4 The User shall be liable to MBUSA in conjunction with these DCS Certificate GTCs according to the statutory regulations. Any further liability by the User toward MBUSA in conjunction with other agreements or services shall remain unaffected.

12.5 In addition to compensation for its own damage, MBUSA can also request compensation for damage caused by the User or the User's vicarious agents or assistants, including subcontractors, to other Group companies by way of performance to MBUSA, as if it were MBUSA's own damages.

13. Rights for handling a DCS Certificate

13.1 MBUSA hereby grants the User only a simple, non-exclusive and non-transferrable right to a DCS Certificate to use the Certificate during the lending period within the scope of the purpose for which it was provided. If the DCS Certificate is issued for a specific person, the usage right is also personally limited to the specific DCS Certificate Holder. The User's subcontractors are entitled to exercise this usage right as defined in these GTCs where this is necessary for the contractual use of the respectively granted certificate.

13.2 It is not permitted to create copies of DCS Certificates, except as far as this is necessary for the contractual use of the respectively issued certificate. Reworking and editing of the DCS Certificates by the User or by commissioned third parties is not permitted.

13.3 Any DCS Certificates and electronic copies that are no longer needed shall be properly destroyed. It must always be ensured that no unauthorized access can take place.

13.4 MBUSA can take appropriate technical measures to prevent non-contractual use. This shall not impair the contractual use of the services.

13.5 Upon request, the User shall permit MBUSA to review whether the User is utilizing the DCS Certificates within the scope of the granted usage rights. The provisions in section 9.5 apply correspondingly.

13.6 Prerequisite for granting rights to DCS Certificates is compliance with these GTCs. In the event of a violation by the User (or by a vicarious agent or assistant) of these GTCs, MBUSA can prohibit further use of the DCS Certificates, in whole or in part, with immediate effect. In the event of a prohibition, MBUSA can request written confirmation from the User that all copies have been deleted or destroyed. The right to assert claims for damages remains unaffected.

13.7 MBUSA can revoke the User's usage right at any time and/or terminate the Framework Agreement and all Individual Agreements without notice period if the User oversteps its usage rights or violates provisions intended to prevent unauthorized use. MBUSA shall in principle set an appropriate grace period for the User first, if this does not pose any disadvantage to MBUSA.

14. <u>Term of the Agreement</u>

14.1 This Framework Agreement shall take effect when it is signed by MBUSA and the User, for an indefinite period of time.

14.2 The term of an Individual Contract for a specific DCS Certificate in principle corresponds to the validity period for this DCS Certificate, which is announced when the certificate is issued. MBUSA and the User can ordinarily terminate an individual agreement in text form without notice period.

14.3 MBUSA and the User can ordinarily terminate this Framework Agreement, in whole or in part, with three months' notice period to the end of a calendar month. Such termination must be declared in writing in order to be valid.

14.4 The right to extraordinary termination for good cause remains unaffected. Good cause for MBUSA particularly exists in the case of any violation by the User (or by a vicarious agent or assistant, including subcontractors) of obligations in connection with confidentiality and security, as well as in the case of an objective suspicion of security or confidentiality violations which the User does not fully dispel in a timely manner after being notified by MBUSA. The right to assert claims for damages remains unaffected.

14.5 Upon cessation of the Framework Agreement or an individual agreement, as well as in the case of a partial or full prohibition of use, the User shall immediately cease any and all use of the affected DCS Certificates and completely delete all DCS Certificates. MBUSA can request the User to provide written confirmation of the deletion or destruction of all copies. The right to assert claims for damages remains unaffected.

15. <u>Data protection</u>

15.1 The User shall conclude any necessary data protection agreements with MBAG regarding the handling of personal data. MBAG is only responsible for data processing in respect of data privacy in the context of the DCS Certificate issuing process and certificate administration where such data processing takes place within MBAG's sphere of influence.

15.2 Neither MBAG nor MBUSA are responsible for data processing within the User's area of responsibility or sphere of influence. Responsibility for collecting and transmitting data to MBUSA for the purposes of Framework Agreements and Individual Contracts, as well as for their performance, shall be borne solely by the User. In this regard, the User is also the controller with regard to the DCS Certificate Holders and DCS Certificate Responsibles.

15.3 The User must comply with Directive (EU) 2016/679 ("General Data Protection Regulation" or "GDPR") as well as other statutory data privacy regulations. A violation of data privacy regulations is also considered a violation of material contractual obligations.

16. Miscellaneous

16.1 Within the framework of its commercial dealings with MBUSA, the User is obliged to desist from all practices which may lead to penal liability due to fraud or embezzlement, insolvency crimes, crimes in violation of competition, guaranteeing advantages, bribery, acceptance of bribes or other corruption crimes on the part of persons employed by the User or other third parties. In the event of violation of the above, MBUSA has the right to immediately withdraw from or terminate all legal transactions existing with the User and the right to cancel all negotiations. The above notwithstanding, the User is obliged to adhere to all laws and regulations applicable to both itself and the commercial relationship with MBUSA.

16.2 The User shall observe the applicable import and export regulations for goods and services on its own responsibility. In the event of an international delivery or service, the User shall bear all applicable customs duties, fees, and other charges. The User shall handle all statutory and official proceedings relating to international deliveries or services on its own responsibility, unless as far as explicitly agreed otherwise.

16.3 The User cannot transfer to third parties any rights or obligations arising from or in connection with the Agreement, or its initiation, without MBUSA's prior consent.

16.4 The User can only offset against MBUSA's claims or assert retention rights if the User's counterclaim from the same agreement is ready for judgement or legally binding.

16.5 Each Agreement concluded according to these conditions shall remain otherwise binding even if single provisions are legally invalid or in the case of regulatory gaps. If a provision should be invalid or incomplete in full or in part, the parties to the Agreement shall immediately strive to achieve the desired economic effect of the invalid or incomplete provision in another, legally permissible, manner.

Annex 1 to Exhibit C

Mercedes Benz Star3 Car-IT Security

Version 1.4

Basic security for DCS certificates

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	20.08.2020	M. Wittiger	Reference to NIST SP 800-57 added.

2. Introduction

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

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

To protect DCS certificates and the respective private keys organizational, procedural and technical controls shall be implemented according to the international information security standard ISO 27001, NIST SP 800-57 key management 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 certificates and keys provided by Mercedes Benz 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 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 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 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 certificates or respective keys or is related to processing DCS 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 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 Mercedes Benz 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 Mercedes Benz (cf. ID#5). Mercedes Benz may ask for a proof of qualification of these technical expert.
4	Relevant systems and applications that are not provided by Mercedes Benz 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 Mercedes Benz (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. Identified vulnerabilities and weaknesses shall be reported to the security manager who will report them to Mercedes Benz.
6	Mercedes Benz 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 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 Mercedes Benz counterpart frequently.
8	Permission to request and access to *personal* DCS 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 certificates or respective keys.
10	Access to keys for personal DCS certificates shall require 2 means of authentication.
11	It shall be transparent to the contractor which user has access to *non-personal* DCS certificates or respective keys. Upon request by Mercedes Benz the contractor shall provide this information to Mercedes Benz.
12	a. Cryptographic keys shall be protected according to state of the art while in transit and at rest. b. Passwords that protect DCS certificates or respective keys shall be configured according to state of the art.

ID	Requirement
13	Idle timeouts shall be configured after which re-authentication is required according to state of the art.
14	Applications handling and storing DCS certificates and keys shall be hardened and patched according to state of the art.
15	Systems handling and storing DCS certificates and keys shall be hardened and patched according to best practice.
16	Systems handling and storing DCS 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 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 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 12 – 14 are met on the diagnostic testing device if ZenZefi is used for certificate management on the respective device.