Microsec Ltd.

General Terms and Conditions for the CCMS V2X PKI Service

Effective date: 14. May 2021.

ver. 1.0

Document History

Version	Description of change	Effective date
1.0	First version	2021-05-14

Table of content

1. Data and Contact Details of the Security Provider

1.1. Name and Address of the Security Provider

Name	Microsec Micro Software Engineering & Consulting Private Company Limited by Shares (hereinafter: the ***Security Provider***)
Company Registration Number	01-10-047218 (registered by: Registry Court of the Metropolitan Regional Court)
Registered seat	H-1033 Budapest, Hungary, Ángel Sanz Briz út 13.
Phone	(+36-1) 505-4444
Website	https://www.microsec.hu, https://www.e-szigno.hu, https://www.v2x-pki.com

1.2. Data protection

1.2.1. Information on data processing prescribed in the Freedom of Information Act and the GDPR (as defined later) are outlined in the Privacy Notice of the Security Provider. The Privacy Notice may be observed on the website of the Security Provider (https://e-szigno.hu/en/privacynotice.html).

1.2.2. The subscriber of the V2X PKI service (hereinafter: the ***Subscriber***) shall use the service under the present General Terms and Conditions (hereinafter: ***GTC***) via a Registration Authority (hereinafter: ***RA***) and the standardised APIs. The Subscriber shall determine the users to be registered having access to the RA, who will be entitled to submit certain requests to the Security Provider on behalf of the Subscriber (primarily in relation to managing the certificates of the Subscriber). These users determined by the Subscriber shall administer the Subscriber's certificates and devices (hereinafter: ***Administrator***) and therefore, may access the RA via a secure channel using personal authentication certificates issued by the Security Provider as trust service provider. The Parties declare that the conditions of accessing the RA (e.g. via a Registration API, individually designed channel of access etc.) are set out in their individual Service Agreement (as defined later).

1.2.3. The Security Provider – in order to guarantee the security of access to the RA and to be able to control any unauthorized activity logs the following data in relation to each access to the RA: (i) all data of the personal authentication certificate of the Administrator, (ii) the exact time of access and (iii) the entire activity of the Administrator carried out when accessing the RA. The Security Provider stores such data for a period of 5 years (statutory limitation period) after each access, in order that it may prove in the future that only authorized users could access the service and that the Security Provider had not violated its obligations towards the Subscriber.

1.2.4. By way of accepting the present GTC, the Subscriber declares having read the Privacy Notice of the Security Provider and gives its express consent to the data processing.

2. The Purpose, Scope and Publication of the GTC

2.1. Purpose of the GTC

2.1.1. The purpose of the present GTC is to lay down the detailed rules for the legal relationship between Microsec Ltd. as the Security Provider providing the CCMS V2X PKI service (hereinafter: ***Service***) and the client ordering such Service, the Subscriber (Security Provider and Subscriber hereinafter separately: ***Party***, together: ***Parties***).

2.1.2. For the sake of clarity, the Parties state that the definition of „Security Provider" has the same meaning as the definition of „V2X PKI Provider", „PKI Provider", or "CCMS Provider" that are also well-known definitions on the V2X PKI market.

2.2. Personal scope

2.2.1. The personal scope of the GTC extends to the Security Provider and the Subscriber, and with respect to certain provisions, to the Administrator, acting as the Subscriber's representative in course of using the Service.

2.2.2. By accepting this GTC pursuant to Section 6:209(1) of Act V of 2013 on the Civil Code, the Subscriber agrees that the Security Provider is entitled transfer the contract under these GTC (i) to his affiliated company or (ii) in the event of acquisition, corporate restructuring or if it transfers its assets in full or substantially to a third party. Such transfer becomes effective by notifying the Subscriber.

2.3. Term of the GTC

2.3.1. This GTC will be valid from the effective date indicated on the front page until revoked or until the effective date of a modified version.

2.3.2. Unless the Parties agree otherwise, the agreement between the Subscriber and the Security Provider regarding the Service will be concluded for an indefinite period of time.

2.4. Services Subject to the GTC

2.4.1. Parties agree that the material scope of these GTC extends only to the CCMS V2X PKI Service.

2.4.2. The Administrators of the Subscriber shall access the RA via a secure channel using electronic authentication certificates, therefore, the Subscriber shall enter into a separate agreement with the Security Provider acting as trust service provider, covering the required authentication certificates. Consequently, the material scope of the present GTC does not cover the following:

a) issuing and maintaining electronic signature and seal certificates as defined in EU Regulation No 910/2014 on electronic identification and trust services (hereinafter: ***eIDAS***),
b) issuing and maintaining authentication and encryption certificates (for user authentication) and further certificates for users other than road side units;
c) license of the software creating and handling electronic signatures and seals,
d) timestamping service.

2.5. Legal background of the Service

2.5.1. The V2X PKI Service has been developed based on (thus compliant with) various standards and specifications; these, for example include the Institute of Electrical and

Electronics Engineering (IEEE)'s WAVE and the European Telecommunications Standards Institute (ETSI)'s ITS standards, such as:

- IEEE Std 1609.2 (IEEE Standard for Wireless Access in Vehicular Environments)
- ETSI TS 102 940 1.3.1 (ITS-S security (PKI) architecture and application groups)
- ETSI TS 102 941 1.4.1 (Trust and Privacy Management)
- ETSI TS 103 097 1.4.1 (Certificate and message structure definitions for C2CPKI)

2.5.2. The V2X PKI Service regulated in the present GTC complies with the following legal regulations:

- Regulation No (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter: ***General Data Protection Regulation*** or ***GDPR***)
- Act V of 2013 on the Civil Code (hereinafter: ***Civil Code***),
- Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter: ***Freedom of Information Act***)

2.6. Publication

Upon releasing the present GTC, it is available only for the Subscribers. The Parties state that the entire content of the GTC shall be treated as trade secret.

3. Contracting based on the GTC

3.1. Service Agreement

3.1.1. The Security Provider and the Subscriber lay down their individual agreement regarding the Service in a separate service agreement (hereinafter: the ***Service Agreement***). Upon signing the Service Agreement, the Subscriber shall accept the provisions of the present GTC and the practice statements of the Service which are: (i) V2X Cooperative Intelligent Transport, Systems ROOT CA Certification Practice Statement; (ii) V2X Cooperative Intelligent Transport, Systems Enrolment Authority Certification Practice Statement; (iii) V2X Cooperative Intelligent Transport, Systems Authorisation Authority Certification Practice Statement (hereinafter together: the CCMS ***V2X PKI Practice Statements***) as binding on itself. The agreement of the Parties is governed jointly by the Service Agreement, the present GTC and the CCMS V2X PKI Practice Statements (hereinafter: the ***Agreement***).

3.1.2. In case the Subscriber and the Security Provider agree to deviate from certain provisions of these GTC, the Service Agreement shall determine all such provisions in detail. The Service Agreement shall also include the wording of the individual agreement of the Parties replacing such provisions of the GTC that will not be applicable to the legal relationship of the Parties.

3.1.3. The Subscriber acknowledges that the entire content of the CCMS V2X PKI Practice Statements is audited and therefore the Security Provider may not deviate from its provisions in course of providing the Service.

4. Description of the Service and the conditions of its use

4.1. Description of the Service

4.1.1. V2X PKI Service is a security framework for providing the safety of vehicle-to-everything communication. In such environments, public key infrastructures (PKI) are used to secure the environment by verifying the participants' permissions with the usage of certificates (hereinafter: ***Certificates***). Microsec V2X PKI Service does this with the most up-to-date cryptographic solutions, including Elliptic Curve Cryptography (ECC) which has more advantage than the widely used RSA algorithm.

4.1.2. Certificates are used to prevent unauthorized parties to interfere with the exchange of data and in order to pseudonymize the communication in a secure way. Certificates can be issued for two types of devices: for On-Board Units (hereinafter: ***OBU***) and Road-Side Units (hereinafter: ***RSU***). The present GTC covers only RSUs which are non-moving units, placed on static devices, such as traffic lights, road signs, etc.

4.1.3. The mechanism of issuing the Certificates is the following. There is a RootCA, that issues CA Certificates for two other authorities, the Enrolment Authority and the Authorization Authority. The Enrolment Authority issues a Certificate, the so-called Enrolment Credential (hereinafter: the ***EC***) that identifies the RSU in the long run. The ECs are required by the Authorization Authorities to issue a different type of Certificate, the so-called Authorization Tickets (hereinafter: the ***AT***), which guarantee the pseudonymity of the OBU/RSU as required by the applicable standards. The Security Provider undertakes to issue both types of Certificates under the present GTC and manage them in accordance with the instructions of the Subscriber, the provisions of the CCMS V2X PKI Practice Statements and the present GTC.

4.1.4. The Service is ISO/IEC 27001 audited, HSM-based Microsec CCMS V2X PKI service, backed by an eIDAS conform qualified trust service environment.

4.2. Technical conditions of using the Service

4.2.1. The Subscriber shall have appropriate technical conditions to access the RA, the details of which are laid down in the Service Agreement.

4.2.2. Administrators of the Subscriber shall have valid electronic authentication certificates to be able to access to RA via a secure channel. It is the task and responsibility of the Subscriber that the Administrators are attributed with the necessary certificates, thus the Security Provider is not responsible if anyone acting on behalf of the Subscriber may not access the RA of the Service due to the lack or failure of the respective authentication certificate. The scope of the Service Agreement does not extend to the authentication certificates to be obtained by the Subscriber. The Subscriber shall conclude a separate agreement for trust services in this regard.

4.2.3. In order to use the Service, the Subscriber must have internet connection and computing devices in conformity with ETSI TS 102 941 1.4.1 and compliant with the Parties' separate agreement regarding the RA requirements.

4.2.4. The Subscriber acknowledges that in order to use the Service, a HSM module approved by the Security Provider shall be obtained. Such HSM module shall be compliant with the requirements of the CCMS V2X PKI Practice Statements and shall serve as the secure hardware device for storing the private keys pertaining to the Subscriber's Certificates. Any interruptions, errors or outages of the Service caused by the non-appropriate operation of the HSM module shall fall within the exclusive responsibility of the Subscriber.

4.2.5. After concluding the Service Agreement, the Subscriber may generate a canonical identifier and canonical key pair for using the Service. The Subscriber undertakes that any and all persons acting on its behalf when using the Service shall handle the canonical identifier, the canonical public key pair and any further identification data and/or password privately and do all that is necessary in order to keep these data safe from any unauthorized persons. In case such data pertaining to the Subscriber (or its individual Administrators) fall into unauthorized hands due to any reasons, then the Subscriber shall be liable for all the resulting damages.

5. Term of Service, availability

5.1. Term of Service

5.1.1. The Service is available on every day of the week 0-24.

5.1.2. The Security Provider deals with the Subscribers' notices, complaints within the working hours and via the contact details as set out in the Service Agreement.

5.2. Availability of the Service

5.2.1. The annual guaranteed availability of the following components of the Service is 99%

- Enrolment Authority service (based on ETSI TS 102 941)
- Authorization Authority service (based on ETSI TS 102 941)
- Distribution Centre service (based on ETSI TS 102 941)

5.2.2. **Planned shutdown**: The Security Provider is entitled to temporarily suspend its Service due to planned maintenance, development, reconstruction works. This period cannot exceed 24 hours per month and 6 hours per occasion. The Security Provider shall announce the planned shutdown at least 24 hours before its start, by sending an email to the contact person of the Subscriber, determined in the Service Agreement.

5.2.3. **Extraordinary outage**: The Security Provider is entitled to carry out maintenance work to counter the threat without prior notice in cases that threaten the data and operational security of the Service and require immediate action. In such cases, the Security Provider shall endeavour to carry out the necessary maintenance tasks with the least possible loss of service. Extraordinary outage count as service gap that shall be taken into consideration when calculating the annual availability.

5.2.4. **Suspended service**: The Security Provider has the right to permanently suspend the Service due to unforeseen and unavoidable external reasons (force majeure) or because entities authorized by law ordered so. In such case the Subscribers shall be informed about the fact that the Service is suspended and the expected duration of the shutdown as soon as possible on the Service's website.

5.2.5. The period of the Planned shutdown and the Suspended service do not count as service gap and shall not be taken into consideration when calculating the annual availability.

6. Responsibility, rights and obligations of the Parties

6.1. Rights and obligations of the Security Provider

6.1.1. The Security Provider shall comply with the terms of this GTC when providing the Service, with the diligence and prudence normally expected from an information technology service provider.

6.1.2. If there are obstacles to use the Service, the Security Provider shall inform the Subscriber as soon as possible. The Security Provider is entitled to refuse or limit its Services – along with notifying the Subscriber – if the Subscriber endangers the security or the availability of the Service.

6.2. The Security Provider’s liability

6.2.1. General Rules of the Security Provider’s liability

6.2.1.1. The Security Provider proceeds towards the Subscriber according to the applicable terms of the Civil Code.

6.2.1.2. In order to determine, document and prove the pecuniary liability, its own liability of any damage caused and the damages caused to it, the Security Provider logs its activities, protects the integrity and authenticity of its log files and retains (archives) them for a long term (5 year from when it was generated).

6.2.2. Exclusion and limitation of the Security Provider’s liability

6.2.2.1. The liability of the Security Provider for any damages suffered by the Subscriber in relation to the Service under the present GTC is limited. The Security Provider’s liability’s maximum extent is the amount of the annual Subscription Fee (as defined later).

6.2.2.2. The Security Provider excludes its liability if the Subscriber does not proceed in compliance with the Service Agreement, the present GTC and the applicable law, thus especially, if the Subscriber does not fulfill the technical conditions of using the Service as prescribed in Section 4.2.

6.2.2.3. The Security Provider may refuse providing the Service to protect its own system and security, if a content uploaded by the Subscriber into the RA is infected with virus and may not be obliged to compensate any damage arising out of the Subscriber having uploaded a content infected with virus.

6.2.2.4. The Security Provider is entitled to limit or refuse access to the Service if the RSU device is compromised, stolen, or deactivated by any reason. In such cases the Security Provider is not liable for the unavailability of the Service.

6.2.2.5. The Security Provider shall not be liable for (i) circumstantial or indirect damages, (ii) loss of profits, (iii) loss or decrease of business opportunities or clients, (iv) loss or decrease of good reputation, (v) loss of data, data theft, data corruption or destruction of data, in case that this is not a result of the Security Provider’s breach of contract or an event within the Security Provider’s sphere of interest, (vi) damage in the data and equipment owned or possessed by the Subscriber, in case that is not a result of the Security Provider breaching the contract between the Parties intentionally or with gross negligence.

6.2.2.6. The Security Provider is not responsible for not fulfilling or not fulfilling timely its obligations under the Service Agreement and the present GTC, if that is a result of such circumstances that fall beyond the reasonable control of the Security Provider (such as natural disasters, war, terrorist activities, malware, pandemic, injury or compliance with any applicable laws or government decrees). The Security Provider makes its best efforts to minimize the effects of such events and to fulfill its obligations not affected by the above circumstances.

6.2.2.7. The limitation and exclusion of the Security Provider’s liability is not applicable in case of personal injury or death caused by the fraud or negligence of the Security Provider, its subcontractors and/or representatives or in case the Security Provider breaches its contractual liability intentionally or by way of damaging human life, the physical integrity or health of others.

6.2.3. Notice of claims against the Security Provider

6.2.3.1. The Security Provider reimburses any damage of the Subscriber caused by the use of the Service after all documents necessary for the decision on the damage claim and evidencing the date and amount of the damage are available.

6.2.3.2. The Subscriber shall send its damage claim in writing to the Security Provider within 30 days from becoming aware of the damage and shall comply with the general obligation to mitigate arisen damages. The Security Provider excludes its liability for any damages in connection with the late notification of the claim.

6.2.3.3. The Subscriber shall act in good faith and fair dealing in connection with its damage claim and shall expressly and clearly evidence the relating circumstances towards the Security Provider.

6.3. Rights and obligations of the Subscriber

6.3.1. The Subscriber is obliged to use the Service according to the effective legal regulations. The Subscriber must ensure that only authorized persons have access to the data and devices necessary for the use of the Service.

6.3.2. The Subscriber has the right to registrate RSUs and submit Certificate requests to the Security Provider.

6.3.3. It is the sole responsibility of the Subscriber if the Service may not be provided due to the Subscriber not having the appropriate technical conditions, access right to the Service, or trust service necessary for using the full scope of the Service.

6.3.4. If the Subscriber causes damage by failing to fulfil its duties set out in this GTC, the Subscriber is responsible for the damage according to the general regulations of the civil law.

6.3.5. In case the Subscriber learns that any certificate data of a Certificate issued upon its request by the Security Provider has changed, it is obliged to immediately report this fact to the Security Provider and initiate the suspension or revoking of the affected Certificate. The Subscriber acknowledges that no Certificate may be used that contains invalid data. The Security Provider fully excludes any and all liability it may have for damages arising out of the fact that a Certificate of the Subscriber contains invalid data.

6.3.6. The Subscriber acknowledges that the Security Provider may only issue such Certificates that comply with the permissions of the Subscriber determined upon concluding the Service Agreement. The Security Provider shall validate the data to be entered on the Certificates according to the CCMS V2X PKI Practice Statements, before issuing Certificates. The Subscriber is liable to notify all changes to the data appearing in a Certificate before such changes are effected. The Subscriber acknowledges that in case a data appearing in a Certificate changes, a new Certificate shall be issued (the RSU shall be reinitialized), because the Security Provider may not modify the data appearing in a Certificate. If the Subscriber learns that a data appearing in a Certificate will change, a notification shall be sent to the Security Provider at such point of time, when the Certificate may still be used for the full length of one AT pre-load period. The concerned RSU shall be reinitialized after the AT pre-load period ends (the length of one pre-load period is defined in the CCMS V2X PKI Practice Statements).

6.3.7. Subscribers shall be obliged—upon being called upon to do so—to cooperate with the Security Provider in the interest of validating the data necessary for issuing Certificates, to make the documents and information the Security Provider requests available to the Security Provider, and to do everything they can to allow the soonest possible completion of such validation.

6.3.8. The Subscriber is obliged to notify the Security Provider immediately of any abnormal operation of the registered RSUs (eg. the device is missing or sending doubtful messages, the key is compromised etc.).

6.3.9. The Subscriber is obliged to control, keep confidential, properly protect and keep in the hardware security module approved by the Security Provider at all times the private key of the Certificates (the private key pertaining to the public key to be included in the Certificate belonging to its subscription, including the key activation data). Should a Subscriber learn that the private key, cryptographic hardware device or the secret codes necessary for device activation of any RSU belonging to its subscription have fallen into unauthorised hands or have been destroyed or otherwise compromised, the Subscriber shall be obliged to notify the Security Provider immediately and initiate the suspension or revocation of the affected Certificate(s). The Security Provider excludes any and all liability it may have for damages arising out of the use of such Certificates.

7. Fees and payment terms

7.1. Fees of the V2X PKI Service

7.1.1. The Subscriber shall pay an annual fee for having access to the Service (hereinafter: the ***Subscription Fee***). The Subscriber shall furthermore pay a registration fee per each RSU registration (hereinafter: the ***Registration Fee***). The Security Provider and the Subscriber may agree in the Service Agreement that the Subscription Fee covers the Registration Fee regarding a given number of RSUs, in such case no separate Registration Fee is payable regarding the number of RSU registrations covered by the Subscription Fee.

7.1.2. In addition to the Subscription Fee and the Registration Fee, the Subscriber shall also pay an annual support fee (hereinafter: ***Support Fee***) for the support of the Service. The amount of the Support Fee depends on the support package chosen by the Subscriber, as outlined below.

7.1.3. The exact amounts of the fees applicable to the Subscriber are determined in the Service Agreement.

7.2. Subscription Fee

7.2.1. The Subscription Fee is the consideration payable by the Subscriber to the Security Provider for the usage of the Service. Upon payment of the Subscription Fee, the Security Provider gives access to the Subscriber to the V2X PKI enrolment and authorisation authorities, including the enrolment, provisioning, bootstrapping and certificate management of the number of RSUs outlined in the Service Agreement.

7.2.2. The Subscription Fee is an annual fee payable in advance for the next 365 days (or in case of a leap year, for the next 366 days) of using the Service (hereinafter: the ***Annual Service Period***). In this period, the Subscriber is entitled to register any number of RSUs via the RA. The Security Provider gives access to the Subscriber to the Service (hereinafter: the ***Access Date***) as set out in the Service Agreement, on the Access Date mutually designated by the Parties. The Security Provider shall issue its invoice regarding the Subscription Fee and the Support Fee for the first Annual Service Period at least 15 days before the Access Date. On the Access Date, the Security Provider is obliged to provide access to the Service, provided that on this day the amount of the Subscription Fee and the Support Fee has already been credited on the Security Provider's bank account. In case the Subscription Fee and the Support Fee have not been credited on the Security Provider's bank account on the Access Date, the Subscriber shall be granted access to the Service within 1 working day as of the day when the amount of the Subscription Fee and the Support Fee are credited on the Security Provider's bank account The Security Provider is entitled to claim the invoiced Subscription Fee and Support Fee as of the Access Date, even if the Subscriber may not actually access the Service upon the Access Date, due to such reasons that fall beyond the Security Provider's control (such as the absence of the appropriate technical conditions on the Subscriber's side or the non-fulfillment of the Subscriber's payment obligations in due time). The Subscription Fee enables the Subscriber to use the Service within the Annual Service Period. On the date when the Annual Service Period ends (the 365th day after the Access Date, hereinafter: the ***Yearly Settlement Date***) the Parties shall settle the amount of RSUs actually registered by the Subscriber within the Annual Service Period (see below in Section 7.3 Registration Fee).

7.2.3. The Security Provider shall issue its invoice regarding the yearly fees, the Subscription Fee and the Support Fee for the following year at least 45 days before the Yearly Settlement Date. In case the Subscriber wishes to maintain the Service for the next year, it shall settle the invoice within the next 15 days.

7.2.4. In case the Subscriber does not wish to maintain the Service for the next Service Year, the Subscriber shall terminate the Service Agreement for convenience, as set out in Section 10.3 of this GTC.

7.2.5. In case the Security Provider does not receive the Subscriber's termination notice until 30 days before the Yearly Settlement Date, the Service Agreement shall remain in force and the invoice regarding the Subscription Fee for the following year shall remain due and payable.

7.2.6. In case the Security Provider receives the Subscriber's termination notice until 30 days before the Yearly Settlement Date, the Service Agreement shall be considered terminated by the Subscriber as of the Yearly Settlement Date. In such case, the Subscriber's access to the Service will be terminated on the Yearly Settlement Date, however, the Parties shall deem such provisions of the Service Agreement and this GTC valid and effective that serve the following purposes: (i) the exact amount of RSU registrations carried out in the Annual Service Period may be calculated, (ii) the applicable Registration Fee and any other outstanding fees payable by the Subscriber may be settled.

7.3. Registration Fee

7.3.1. The Registration Fee covers the following services: Road-Side Unit device enrolment, provisioning enrolment credentials and authorization tickets, bootstrapping and certificate management. The Registration Fee is payable yearly once, based on the RSUs that have been registered within the Annual Service Period (hereinafter: ***Total Annual RSU Registrations***). For the sake of clarity, the Parties declare that when calculating the Total Annual RSU Registrations, the Security Provider takes into account the total number of *registrations* carried out by the Administrators of the Subscriber, and not the number of RSUs registered in the Annual Service Period, whereas such RSUs that have been registered in a previous Annual Service Period, but are still actively registered in the actual Annual Service Period, shall be considered as registrations as well. Therefore, in case the same RSU is registered more than once within one Annual Service Period, all registrations pertaining to this RSU are included in the Total Annual RSU Registrations.

7.3.2. Upon the Yearly Settlement Date, the Security Provider shall take account of the Total Annual RSU Registrations carried out on behalf of the Subscriber. The Security Provider shall send a list of the Total Annual RSU Registrations to the Subscriber, together with the pertaining invoice, within 30 days as of the Yearly Settlement Date.

7.3.3. In case the Security Provider and the Subscriber had agreed in the Service Agreement that the Subscription Fee covers the Registration Fee of a given number of RSUs, the Security Provider shall not take into account the Registration Fee of these RSUs, when issuing its invoice regarding the Registration Fee.

7.3.4. In case the Service Agreement is terminated, the Security Provider shall inform the Subscriber of the total number of RSUs that have been registered on behalf of the Subscriber until the date of termination (not previously settled between the Parties) and issue its respective invoice within 15 days as of termination.

7.4. Support Fee

7.4.1. The Parties agree that the yearly initial Support Fee is payable in advance, together with the Subscription Fee, under the same payment conditions.

7.4.2. The Parties agree that changing the Support Package available to the Subscriber as outlined in Section 8.1, shall not qualify as such modification of the Service Agreement that has to be made in writing. Upon confirming the change of the Support Package via email, the Security Provider shall be entitled to issue its pertaining invoice to the Subscriber.

7.5. Consultation Fee

7.5.1. The Security Provider provides the opportunity for the Subscriber to consult with its PKI experts on specific technical issues in connection with (i) creating the necessary technical background of the Service at the Subscriber (especially development consultation regarding the Registration API), (ii) the launch and regular operation of the Service and (iii) any other such expert issues that do not fall within the general support of the Service as defined in Chapter 8 (hereinafter: ***Consultation Services***).

7.5.2. The method of providing Consultation Services is primarily online. In case any Subscriber wishes that the PKI experts of the Security Provider provide on-premise Consulting Services, all relating costs (especially travel and accommodation) shall be borne by the Subscriber.

7.5.3. As Consultation Services, the PKI experts of the Security Provider may provide PKI training for the colleagues of the Subscriber (in e.g. the following topics):

(i) Basic cryptography and PKI knowledge, PKI building blocks, the role and the processes of a Certificate Authority,

(ii) The anatomy of an electronic signature creation, validation, legal framework, use cases

(iii) Encryption, authentication, attribute certificates.

7.5.4. The fee of the expert level Consultation Services requested by the Subscriber shall be paid by the hour, based on the hourly fee outlined in the Service Agreement. The Security Provider takes notes of the conducted Consultation Services and informs the Subscriber upon every 20 hours of completed Consultation Service. The Security

Provider is entitled to invoice the rendered Consultation Services to the Subscriber every month.

7.6. Unilateral right to increase fees

7.6.1. Microsec reserves the right to unilaterally increase the fees payable under the present GTC, once in a year, in course of the yearly fee settlement process as outlined above in Section 7.3.2. The maximum amount of the unilateral increase of the payable fees may not exceed the volume determined in the Service Agreement. The Security Provider informs the Subscriber of the amount of the increased fees upon providing the Subscriber with the invoice for next year's Subscription Fee. In case the Subscriber does not wish to maintain the Service Agreement under the modified pricing conditions, the Subscriber shall terminate the Service Agreement with termination for convenience, as outlined in Section 10.3.1. The Security Provider declares that in case it does not exercise its right to unilaterally increase fees for the next Annual Service Period, this shall not be considered as a waiver of rights in this regard.

7.7. Payment conditions

7.7.1. By way of accepting the present GTC, the Subscriber expressly and irrevocably agrees to the Security Provider issuing electronic invoices.

7.7.2. The Subscriber shall notify the Security Provider if it has not received a due invoice or if the received invoice has not been issued properly.

7.7.3. The invoices issued by the Security Provider shall be settled within 15 days as of issuance. The invoice is considered to be settled if the invoice amount is credited on the bank account of the Security Provider indicated on the invoice.

7.7.4. In case the Agreement is terminated, the Security Provider does not refund already performed payments, unless the Agreement is terminated due to such reasons that fall within the interest of the Security Provider.

7.7.5. The Subscriber shall pay for the use of the Service, even if it claims that such persons used the Service on its account, who have not been authorized to do so by the Subscriber. In such case, the Subscriber shall settle all service fees invoiced by the Security Provider, as long as the Security Provider or the Subscriber does prohibit the access of such unauthorized persons to the Service. The Security Provider denies access to the Service upon request of the Subscriber within 1 working day.

7.7.6. The Security Provider may issue invoices in monthly or yearly billing periods, or on an occasional basis, depending on the type of fee (the Subscription Fee and the Registration Fees are invoiced once in a year, while the Support Fee and the Consultation Fee may be invoiced several times in course of the Service Year, based on the requests of the Subscriber).

7.7.7. Upon the termination of the Agreement, the outstanding fees will be invoiced in the next billing period of the Security Provider, proportionally. In case of fees payable on an occasional basis, the outstanding fee will be invoiced within a reasonable period of time.

8. Use and conditions of the Support service

8.1. Support Packages

8.1.1. The Security Provider provides technical assistance to the Subscriber related to the Service (hereinafter: ***Support***), in exchange of the Support Fee. The Service requires the Support of the Security Provider and therefore, it is not possible to conclude such Service Agreement that does not cover the Support of the Service and the pertaining fees.

8.1.2. Support is only available in packages (hereinafter*: **Support Package(s)***). The different Support Packages contain the same level (quality) Support service, however, the quantity of the Support (the working hours of the Security Provider's staff providing the Support service, hereinafter: the ***Support Hours***) differs. The Subscriber is obliged to choose a Support Package upon concluding the Service Agreement, however, the Subscriber is entitled to increase the number of Support Hours at any time and thus, choose a different Support Package. The detailed rules of the different types of Support Packages are outlined in the Service Agreement, in particular the number of available Support Hours/year, and the hourly fee of the Support.

8.1.3. The Security Provider notifies the Subscriber after every 8 hours of used Support. If the number of Support Hours exceeds the package limits, the Support Package is automatically upgraded to the next available Support Package providing a larger number of Support Hours, unless it is expressly prohibited by the Subscriber, by way of rejecting the pertaining invoice received by the Security Provider. The Subscriber acknowledges that the Security Provider shall not provide any further Support until the Support Fee of the upgraded Support Package is not settled in advance.

8.1.4. The Parties agree that any issue (question, problem or reports of errors - together hereinafter: ***Support Notification***) that is reported by the Subscriber to the Security Provider – when learned by the Subscriber – shall be considered as a started Support Hour.

8.2. Level of the Support

8.2.1. The Support is an expert-level support (Level 3), provided by the Security Provider to Subscriber. In the Service Agreement the Parties may agree that the Security Provider may provide technical level support (Level 2) to the Administrators of the Subscriber. Description of support levels:

Level 1 – End user support - The initial support level responsible for basic customer issues. Typically, support obligations are to gather the customer's information and to determine the customer's issue by analyzing the symptoms and figuring out the underlying problem. This information needs to be recorded into the issue tracking or issue logging system. This information is useful to analyze the symptoms to define the problem or issue.

Level 2 – Customer support - Support is a more in-depth technical support level than Level 1 and typically involves personnel that are more experienced and knowledgeable on a particular product or service. Level 2 support is knowledgeable enough to assist Level 1 personnel in solving basic technical problems and for investigating elevated issues by confirming the validity of the problem and seeking for known solutions related to these more complex issues.

Level 3 – Partner support - Support typically involves expert level troubleshooting and analysis methods. The Level 3 personnel are experts in their fields and are responsible for not only assisting Level 1 and Level 2 but also with the research and development of solutions to new or unknown issues. Upon encountering new problems, Level 3 personnel must first determine whether or not to solve the problem, or first to produce a workaround. If it is determined that a problem can be solved, this group is responsible for designing and developing one or more courses of action, evaluating each of these courses in a test case environment, and implementing the best solution to the problem.

8.2.2. The Subscriber acknowledges that in the framework of Level 3 Support, consultation and Support services are available for such IT experts of the Subscriber, who are equipped with the suitable PKI knowledge basis. Level 3 Support typically requires expert-level debugging and analysis methods.

8.2.3. The Parties agree that the following are not included in the Support:

- making the IT systems of the Subscriber suitable for using the Service,
- development and integration required for using the Service,
- investigation and correction of any problems that may have occurred at the Subscriber due to a change in the operating system or any component thereof,
- troubleshooting of software conflicts,
- correction of other errors that are not a result of the malfunction of the Service,
- assistance with configuring the environment (operating system, application) running the Service,
- data or system recovery due to a virus infection,
- backup scan,
- investigation and correction of a problem due to third party intervention,
- investigation and resolving incidents due to a hardware or network problem.

8.2.4. The Subscriber is obliged to indicate in the Service Agreement the names and contact details of up to 5 employees who are entitled to request Support. Subscriber is entitled to change the persons authorized to request Support at any time, by notifying the Security Provider 5 days prior to such change.

8.2.5. The Subscriber is entitled to send Support Notifications to the Security Provider at any time (0-24h). The Subscriber expressly acknowledges and accepts that the deadline for answering the Support Notifications starts on workdays, in the opening hours of the Security Provider (8 a.m. to 16 p.m.).

8.2.6. Within its opening hours, the Security Provider is obliged to shortly confirm the receipt of a Support Notification to the Subscriber. If the Support Notification is a report of an error, the Security Provider specifies the category of the error in the confirmation message.

9. Reporting, handling complaint errors and complaints

9.1. Error reporting process

9.1.1. The Subscriber shall promptly notify the Security Provider of any clearly identifiable errors of the Service and provide adequate support to the Security Provider in resolving the error (especially answering the queries of the Security Provider in connection with experiencing the error, sending error messages and other evidences expediating the debugging and fixing process etc.).

9.1.2. Errors of the Service shall be reported via the electronic contact details / the platform for Support requests, as determined in the Service Agreement. The Parties may agree in the Service Agreement that Support via telephone is also available to the Subscriber, under the conditions determined in the Service Agreement. If the Service Agreement includes the possibility of using telephone assistance, the Subscriber may only contact the Security Provider via telephone to report such errors that qualify as Critical and Serious Errors (as defined later). Error reports communicated via telephone must be confirmed electronically in writing to the Security Provider, within a maximum of 1 working day of the telephone call.

9.1.3. After the Subscriber reports the error, the Security Provider shall begin troubleshooting within the appropriate time frame, according to the level of the error. If the Subscriber's cooperation is required to correct the error, this period shall start from the Subscriber's availability.

9.1.4. The error report provided by the Subscriber must include:

a) the time when the error occurred or was detected,
b) the exact name of the function or service (e.g. EA, AA, DC (Distribution Center)) affected by the error,
c) configuration data of the device and the sent request (including identifiers/certificates, messages, request hash values),
d) a detailed description of the error (including any relevant log files, statistics, status messages, error codes, and debug messages, and similar information),
e) the impact and extent of the problem (e.g. whether critical data, data access or use of the Services are at risk),
f) the steps already taken to identify and remedy the problem,
g) the last interventions that can be associated with the occurrence of the error (configuration change, administrative steps, cabling, etc.),
h) the name and contact details of the technical contact person (eg. operator, on-call system administrator, operator) acting on behalf of the Subscriber during the troubleshooting.

9.1.5. The Subscriber shall be liable for damages resulting from the late reporting of the error and the failure to report the error, including for not providing the information outlined above necessary to detect and correct the error.

9.1.6. The Security Provider shall investigate the error detected by the Subscriber after the error is reported, within the deadline specified below, and shall inform the Subscriber of the result, which may be as follows:

a) the rectification of the error is completed,
b) the error was not detected during the test,
c) the error occurred for a reason within the Subscriber’s interest,
d) the Subscriber is not entitled to request the correction of the error, in particular because the Service Agreement or the present GTC does not include the correction of the specific type of error.

9.2. Deadlines for troubleshooting and categories of errors

9.2.1. The Security Provider shall start correcting the error in question according to the following deadlines:

a) In case of a Critical Error, the deadline is a maximum of 2 working days.
b) In case of a Major Error, the deadline is a maximum of 5 working days.
c) For all other errors (Minor), the deadline is a maximum of 15 working days.

9.2.2. Categories of errors:

a) **Critical Error:** An error that prevents using the Service or a critical function of the Service, basic operation of the function is not possible, using the Service can only continue after repair. There is no suitable way to avoid the error.
b) **Major Error:** A system error that prevents the execution of a specific function of the Service. The operation of other functions of the Service is not affected by the error.

There is a workaround that allows the Service to continue to be provided until the error is fixed.

c) **Minor Error:** Form, appearance, comfort deviations from the specification that do not affect the execution of Service functions / processes. It does not prevent the Subscriber from using the Service.

d) **Recurring Error:** An error that the Security Provider has corrected previously but it reappears. If the recurring error was previously Critical or Serious, its rating is equivalent to Critical or Serious, if the recurring error was previously considered Slight Error, its rating is equivalent to Slight.

9.2.3. The error is considered to be fixed if its status is fixed within the error reporting electronic system indicated in the Service Agreement / if the Security Provider reports via email to the Subscriber that the error is fixed.

10. Amendment and Termination of the Agreement

10.1. Amendment of the Agreement

10.1.1. The Agreement of the Parties may be amended jointly by way of modifying the Service Agreement or unilaterally by the Security Provider, by way of modifying the present GTC or the CCMS V2X PKI Practice Statements.

10.1.2. The Subscriber is obliged to notify the Security Provider of all changes in the contact details or billing data previously provided to the Security Provider, within 15 days as of such change, via the dedicated e-mail address determined in the Service Agreement. The Security Provider shall not be liable for any such damages that arise due to the Subscriber not notifying the Security Provider of such changes without any undue delay.

10.1.3. The Subscriber is not entitled to transfer its rights based on the Service Agreement and the present GTC to a third party, without the previous written consent of the Security Provider.

10.2. Amendment to the GTC

10.2.1. The Security Provider is entitled to amend the GTC unilaterally. The Security Provider is obliged to notify the Subscriber if there is any such amendment, at least 30 days before entry into force.

10.2.2. If the Subscriber does not accept the amendment to the GTC, the Subscriber may terminate the Agreement within 30 days as of the notification of the amendment, except in the following cases:

a) in case of introducing a new service, function or feature, if it does not adversely affect the conditions relating to already existing Services,

b) in case of expanding the Services, if it does not represent an extra burden on for the Subscriber,

c) in case of a change in the legal environment, a governmental authority’s decision or such change in the economic and/or technical circumstances, as a result of which the Security Provider can only provide the Service for the Subscriber on different terms than before, if it does not represent an extra burden for the Subscriber;

d) if the Security Provider’s address, telephone number and opening hours change,

e) in case of corrections to the GTC made merely for the sake of clarity, which cannot be regarded as modifications to content,

f) in case the conditions of using the Service change in such way, which are exclusively beneficial for the Subscriber.

10.3. Termination for convenience

10.3.1. Considering that the Service under the present GTC may only be used in exchange for an annual Subscription Fee, the Service Agreement may only be terminated with the effect of the Yearly Settlement Date, as defined in Section 7.2.4. In case the Subscriber wishes to terminate the Service Agreement with an effective date earlier than the Yearly Settlement Date, the Security Provider does not refund the already paid Subscription Fee and Support Fee.

10.3.2. The termination period applicable to both Parties is 30 days, beginning on the day when the termination notice arrives to the other Party.

10.4. Termination for cause

10.4.1. In case of material breach of contract, the other Party shall have the right to terminate the Service Agreement — subject to providing an explanation — with immediate effect.

10.4.2. It shall be considered a material breach of contract if the Subscriber jeopardies the security or availability of the Service. In case the Subscriber does not settle any fees payable under the Service Agreement within 30 days as of the expiration of the payment deadline, the Security Provider (simultaneously with calling upon the Subscriber to fulfil its payment obligation, with providing an additional deadline of 15 days) suspends the Service, meaning that the Subscriber will not be able to register any further RSUs after the suspension. In case of such suspension, the already issued Certificates of the Subscriber will not yet be revoked. In case the additional deadline granted in the payment notice expires without the Subscriber settling its outstanding fees, the Security Provider sends a second payment notice, warning the Subscriber that in case the outstanding fees will not be settled within 15 days after sending the payment notice, all Certificates pertaining to the Subscriber will be revoked. After the expiration of the extended payment deadline without the Subscriber settling its outstanding fees, the Security Provider terminates the Service Agreement with immediate effect and revokes all Certificates of the Subscriber.

10.4.3. It shall be considered a material breach of contract, if the Security Provider fails to assure the availability of the Service as stipulated in this GTC or if the Security Provider violates any other requirement related to the Service prescribed in any other legislation.

10.5. General rules of termination

10.5.1. Termination of the Service Agreement shall be made in writing. Within the interpretation of the present Chapter 10, an electronic letter shall be considered to fulfil the written form if the other Party has confirmed its receipt. In case the termination notice is sent via courier or postal services, the termination notice shall be sent via registered mail, requesting an acknowledgement of receipt. In case the terminating Party does not receive an acknowledgement of receipt because the other Party was not found at its address by the courier or the postal services or rejected to receive the consignment, the termination notice shall be considered delivered on the day of the second attempt of dispatch.

10.5.2. In case the Service Agreement between the Subscriber and the Security Provider terminates due to any reason, the Subscriber (and any Administrators acting on behalf of the Subscriber when using the Service) shall immediately stop using the Service. In such case, all certificates pertaining to the Subscriber under the present GTC will be immediately revoked as of the date of the termination. The Security Provider excludes all liability resulting from the Subscriber further using such Certificates after the termination of the Service Agreement that (i) had been previously revoked by the Security Provider (Enrolment Credentials) and (ii) that belong to the EC owner (Authorization Tickets). It is the Subscriber's liability and responsibility to delete all Authorization Tickets after such termination.

11. Miscellaneous

11.1. Applicable law, handling legal disputes

11.1.1. The Parties hereby agree that to their Agreement, the laws of Hungary shall apply.

11.1.2. The Parties agree that to their legal relationship established based on the Service Agreement and this GTC, only this GTC applies, therefore no such custom or condition or shall become part of their legal relationship that the Parties applied in their previous business relationship.

11.1.3. The Security Provider and the Subscriber hereby stipulate the exclusive jurisdiction of the Budapest 2nd and 3rd District Courts with regards to their legal relationship based on this GTC.

11.2. Confidentiality

11.2.1. The Parties acknowledge and consider binding on themselves that all data, facts and any other information they learned, acquired or came to possess in relation to each other's activity, especially affecting the other's business activity, economic, legal and financial situation that have not yet become public domain, shall be treated confidentially as business secret and shall not be shared with or made available to third parties. The Subscriber acknowledges that the content of the Service Agreement and the present GTC shall also qualify as business secret.

11.2.2. The confidentiality undertaking of the Parties shall remain in full force and effect for an indefinite period of time, even after the Service Agreement is terminated.

11.2.3. It shall not qualify as breaching the above confidentiality undertaking, if any of the Parties discloses information qualifying as business secret due to its obligation to provide information prescribed by the law or if the owner of the data had previously given its consent in writing to revealing such information.

11.3. References

11.3.1. The Security Provider is entitled to use the name of the Subscriber and the fact of providing the Service as outlined in the Service Agreement in course of its promotion and marketing activities. Indicating the name of the Subscriber and the fact that the Security Provider provides the Subscriber with the V2X PKI Service shall not qualify as breach of the confidentiality undertaking under this GTC.

11.4. Notifications

11.4.1. Declarations and notifications in connection with the Service Agreement shall be sent to the address of the Security Provider and the Subscriber laid down in the Service Agreement, unless the present GTC stipulates it otherwise.