Terms and Conditions of Use Swisscom ITSF Trust Service, Selected Signing Service (advanced and qualified electronic signatures)

Terms and Conditions of Use for the use of the Swisscom ITSF trust service with advanced and qualified certificates for advanced and qualified electronic signatures (Swisscom ITSF certificate class "Saphir and Diamant")

1 Scope of these Terms and Conditions of Use

These Terms and Conditions of Use shall apply in the relationship between you and Swisscom IT Services Finance S.E, PKI Dienstleistungen, Modecenterstrasse 17/Unit 2, 1110 Vienna, Austria, company number 378965b (hereinafter referred to as "Swisscom ITSF") for your use of the Swisscom ITSF trust service with advanced and qualified certificates for advanced and qualified electronic signatures.

2 Swisscom ITSF's Services

2.1 Certification service in general

For issuing qualified certificates for electronic signatures and electronic seals, Swisscom ITSF is an accredited trust services provider in Austria pursuant to the EU Regulation No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) and the Austrian Signature and Trust Services Act (SVG) and is audited by a confirmation body and supervised by the SVG supervisory body. For your trust services with advanced certificates, Swisscom ITSF provides trust services in accordance with internationally recognised technical standards.

In general, the trust service is provided in accordance with the Swisscom ITSF certificate policy in its then current version. This certificate policy – Certificate Policy (CP/CPS) for the issuance of "Diamant" (Diamond) class certificates (qualified) and "Saphir" (Sapphire) class certificates (advanced) – form an integral part of these Terms and Conditions of Use. You can view and download the document online at www.swissdigicert.ch/download_docs (in the "EU" section).

As part of the trust service, Swisscom ITSF creates a digital certificate which includes personal information about you. Depending on the subscriber application, a distinction is made between certificates using actual names and certificates using a pseudonym (see section 7.3). Swisscom ITSF links this digital certificate with the file which you sign electronically (e.g. a PDF document). The electronic signature on the document is thereby assigned to you as an individual, just as if it were signed in your own hand, where the writing of the name on the document is assigned to the individual signing it. The result is that third parties can also rely on the electronic signature and on the information contained in the digital certificate.

In each case, depending on the type of signature offered by the subscriber application (see section 3 in this regard), either an advanced electronic signature is created pursuant to Article 3 point 11 of the eIDAS Regulation or a qualified signature pursuant to Article 3 point 12 of the eIDAS Regulation is created. No other type of use of the digital certificate is permitted in connection with the use of the trust service in accordance with these Terms and Conditions of Use ("limitation of use").

2.2 Identity verification process and retention of the information

Swisscom ITSF or the registration authority appointed by Swisscom ITSF checks your identity in the identity verification process. For qualified electronic signatures, this is done by means of your passport or official photo ID in personal contact or by means of a certified, equivalent process in which personal presence can be dispensed with.

Depending in each case on the actual organisation of the identity verification process, you may be requested in the verification process for advanced electronic signatures to also submit other documents than those required for qualified electronic signatures.

The validity period of your identity verification is a maximum of five years. However, for qualified electronic signatures the validity period is linked to the validity period of the official identity document submitted by you, which may be shorter.

Based on your identify verification process for qualified electronic signatures, you may also create advanced electronic signatures in accordance with these Terms and Conditions of Use where the subscriber application used by you offers different types of signatures. However, not every identity verification process for advanced electronic signatures can also be used for the superior grade signature level of the qualified electronic signature.

Swisscom ITSF registers and files the personal information about you which is collected in the identity verification process in accordance with the applicable regulations. The handling of your data is described in section 6 of these Terms and Conditions of Use.

2.3 Issuance of certificate and keys, creation of signature, certificate revocation

Swisscom ITSF creates the advanced or qualified certificate and the cryptographic pair of keys for the signing process on a special server (Hardware Security Module, HSM). The advanced or qualified certificate is a certificate which assigns to you the public key of the asymmetrical cryptographic pair of keys. You alone have the activation data which allows you to use the private key by using an authentication method associated with your identity (e.g. bank app, Mobile ID app, Password/ SMS authentication process), see also in this regard sections 3 and 4 of these Terms and Conditions of Use). As soon as you enter the activation data after

being requested to do so, Swisscom ITSF creates the advanced or qualified electronic signature for you.

Swisscom ITSF creates a certificate for you with a maximum validity period of three years.

Should Swisscom have to revoke the signature certificate due to insufficient algorithms, the applicant for this certificate will be informed and receive an offer for a new certificate with sufficient cryptological protection.

2.4 Verification of the electronic signature

The Swisscom ITSF trust service allows the validity of the electronic signature to be validated. Third parties also (often referred to as the "relying party") can validate the validity of your electronic signature (e.g. for qualified electronic signatures on the website www.signatur.rtr.at/de/vd/Pruefung.html).
The information provided in section 5 of these Terms and Conditions of Use must be noted concerning the legal effects of the different electronic signatures.

2.5 Availability

Swisscom ITSF shall endeavour to provide the trust service continuously. Swisscom ITSF shall not, however, be liable for ensuring that the selected signing service is constantly available. Swisscom ITSF may limit the availability temporarily if this is necessary, for example, with regard to capacity limits, or the safety or integrity of the servers, or to perform technical maintenance or repairs and this is for the purpose of providing the services properly or improving them (maintenance work). Swisscom ITSF shall endeavour in this process to take account of the interests of the users of the trust service.

3 Preconditions of use

You have an adequate understanding of digital certificates and of advanced and qualified electronic signatures.

You use a device and log in to an internet portal or an application which allow the Swisscom ITSF trust service to be used (so-called “subscriber application”). For example, it may be your employer's accounting software or your bank's or insurance company's internet portal. The terms and conditions of the subscriber application used by you may result in limitations in the use of the trust service. In particular, the subscriber application used by you determines whether you can create advanced or qualified electronic signatures. The subscriber application also determines whether you go through a one-time identification process for each electronic signature (one-time signature), or whether you can create several electronic signatures for a certain period of time after the identification process. The linking of the subscriber application to the Swisscom ITSF trust service is the subject of a separate agreement (Selected Signing Service Agreement).

You have an approved means of authentication which can be used for confirming your intention to sign (e.g. a mobile phone). Possible multi-factor authentication methods include, e.g. a bank app, Password/SMS Authentication or Mobile ID app or other approved signature authentication methods. The actual signature authorisation results from the connection of the subscriber application used by you.

You acknowledge that violations of the confidentiality and cooperation obligations agreed with your organisation may also constitute a violation of legal provisions that may result in criminal prosecution. This relates, for example, to business secrets.

4 Your cooperation obligations

You undertake as part of the identity verification process to provide Swisscom ITSF and/or the registration authority with complete and true information.

You undertake that, when using secret passwords (where the use of such passwords is envisaged as a means of communicating your intentions), you shall not use any data relating to your personal details (date of birth or the like). You may not disclose any records of your personal password to any other person. These must be stored securely and separately from your mobile phone or encrypted and protected against access by third parties.

If, for example, your mobile device, your SIM card and/or the personal password which you have to provide in the authentication process has been stolen or if you know or suspect that another person has acquired knowledge of it (compromise), you undertake to do the following:

- You immediately stop creating signatures,
- You immediately arrange for invalidation of the certificate and
- If necessary, you change the access data (e.g. bank app, mobile ID PIN or password) and you block your SIM card if necessary.

You also undertake to arrange for invalidation of the certificate if your name, your nationality or other personal attributes change.

You may arrange for invalidation with the registration authority or with Swisscom ITSF pursuant to the procedure specified in the certificate policy.

As soon as there are any changes to a device used for authentication or to your identity data, you shall inform your registration authority or Swisscom ITSF directly of these changes.

You undertake to take every reasonable and readily available opportunity to protect your device and/or your mobile phone used for authentication or signature from attacks and malware ("viruses", "worms", "Trojan horses" and the like), particularly through using software from an official source that is continually updated.

You undertake to check the electronic signatures after they have been created in accordance with section 2.4 of these Terms and Conditions of Use and to promptly report any discrepancies in the digital certificate to Swisscom ITSF.

5 Legal effects of the electronic signature

The trust service in accordance with these Terms and Conditions of Use creates in each case either an advanced electronic signature pursuant to Article 3 number 11 of the eIDAS Regulation or a qualified electronic signature in accordance with Article 3 number 12 of the eIDAS Regulation.

The subscriber application (see in this regard section 3 of these Terms and Conditions of Use) used by you to reach the trust service determines the type of signature (advanced or qualified electronic signature) for each signature process. Swisscom ITSF has no influence on this choice.

Further, the subscriber application used by you to reach the trust service can either have a qualified time stamp associated with the advanced or qualified electronic signature at the trust service, or the time stamp may be dispensed with. Swisscom ITSF has no influence on this choice. An electronic signature is therefore created either with or without a qualified time stamp depending on the setting for the access to the Swisscom ITSF trust service. In verifying the signature (see in this regard section 2.4 of these Terms and Conditions of Use) you can check to see whether or not the electronic signature is associated with a qualified time stamp.

A qualified electronic signature fulfils the legal requirement of writing in the sense of § 886 of the Austrian General Civil Code. In principle, a qualified electronic signature has the same legal effect as a handwritten signature. However, other legal formal requirements, in particular those which provide for the involvement of a notary or a lawyer or in connection with testamentary dispositions, as well as contractual agreements on the form shall remain unaffected. Depending on the particular situation, certain documents require a handwritten signature in order to be legally effective.

An advanced electronic signature does not satisfy the legal requirement of written form. The legal requirement of a handwritten signature can as a matter of principle only be replaced with equivalent effect by a qualified electronic signature, which must not be confused with an advanced electronic signature based on an advanced certificate in accordance with these Terms and Conditions of Use. Depending on the situation, certain documents therefore require a handwritten signature or a qualified electronic signature in order to have the intended legal effects.

It is your responsibility before using the trust service to determine your requirements and the legal effects of the qualified electronic signature or the advanced electronic signature in this context.

You acknowledge that the advanced or qualified electronic signatures created with the Swisscom ITSF trust service may have different, possibly less extensive effects under the law of a country other than Austira and that requirements as to form (such as the written form requirement) might not be met.

The use of certain technical algorithms is also subject to statutory restrictions in certain states. It is your responsibility to investigate the circumstances in this regard beforehand.

The inclusion of additional information in a digital certificate (specific attributes such as, for instance, right of representation for your employer) is purely declaratory, with the existence of an attribute and its legal effects governed by the applicable law (agency law, corporate law etc.) and not within the scope of Swisscom ITSF's influence or responsibilities. Swisscom ITSF shall only be responsible in this context for verifying evidence of an attribute at the time when the identity is verified using the documentary evidence requested by Swisscom ITSF. Specific attributes in the digital certificates do not reflect all possible situations under civil law (collective signing authority, signing authority only in special cases etc.).

6 Duration

Taking account of the preconditions of use pursuant to section 3 of these Terms and Conditions of Use, you may use the trust service using an authentication method deposited at the time of registration in accordance with these Terms and Conditions of Use for a maximum period of eight years.

7 Handling of your data

7.1 General, Privacy Statement

Swisscom ITSF collects, stores and processes only data which is needed to provide the trust service. Handling of the data shall be governed not only by the applicable laws but also by the certificate policy referred to above in section 2.1 of these Terms and Conditions of Use.

For the provision of the trust service Swisscom ITSF involves Swisscom (Switzerland) Ltd., domiciled in Switzerland. Swisscom (Switzerland) Ltd. operates the IT-systems for providing the trust services and these systems are located in Switzerland. The advanced or qualified certificates are thus issued on servers in Switzerland. Swisscom (Switzerland) Ltd. is therefore processing data in Switzerland, which is carried out on behalf of Swisscom ITSF. Swisscom ITSF has concluded the necessary data protection agreements with Swisscom (Switzerland) Ltd.

The handling of your data is further governed by the privacy statement for use of the trust service, which can be accessed at trustservices.swisscom.com

7.2 Identity verification documentation

For the purpose of creating the digital certificate and to maintain the verifiability of the trust service, the registration authority acting for Swisscom ITSF or Swisscom ITSF itself collects and stores the following data about you (to the extent this has been provided by you in the identity verification process in accordance with section 2.2 of these Terms and Conditions of Use):

- A copy of the relevant pages of the identity document submitted by you (passport, identity card, possibly other documents according to section 2.2. if only advanced electronic signatures are to be created) with the information contained therein (in particular: gender, first names, last name, date of birth, valid date of identity document, nationality)

- Information contained in the identity document (in particular: gender, first names, last name, date of birth, valid date of identity document, nationality)
- Personal used means of authentication (e.g. mobile phone number)
- Other information and documents provided by you in the identity verification process (such as residential address, email address, extracts of Commercial Register, powers of attorney or other documentary evidence concerning specific attributes)

If the identity verification process is conducted by video-chat, the following data shall additionally be captured and stored:

- Photograph of you from the video call
- Photographs of the identity document submitted by you
- Audio recording of the video call
- Technical information (e.g. IP address) of the device used by you

7.3 Digital certificate

Based on the data which has been provided by you and collected in the identity verification process, Swisscom ITSF shall at the request of the subscriber application and with your stated consent issue an advanced or qualified certificate containing the following information concerning you, if the subscriber application requires the use of actual names:

- First names, last name
- Two-digit ISO 3166 country code
- Additional information e.g. to ensure the uniqueness of the digital certificate:
- Name of company
- E-mail address
- Number of the identity document presented

If the subscriber application requires the use of a pseudonym:

- Pseudonym
- Two-digit ISO 3166 country code
- Registration authority responsible for verification of identity
- Time of issuance of digital certificate

The digital certificate is included in the electronically signed file after completion of the signing process. Anyone in possession of the digitally signed file may view the aforementioned information from the digital certificate at any time. This enables third parties to review personal information about you and to also see that Swisscom ITSF as a trusted trust service provider guarantees the certification of this data and the signing process.

7.4 Data after completion of the signing process

The registration authority acting for Swisscom ITSF or Swisscom ITSF itself shall retain the data described in section 7.2 for the duration specified in section 6 of these Terms and Conditions of Use to enable you to use the trust service. Swisscom ITSF (where applicable: supported by the registration authority) is further obligated by law in the case of qualified electronic signatures to retain various data concerning the identity verification process, the digital certificate and the signing process for 30 years from expiry or invalidation of the certificate. In the case of advanced electronic signatures, in accordance with its certificate policy, Swisscom ITSF retains various data concerning the identity verification process, the digital certificate and the signing process for at least 7 years from expiry or invalidation of the certificate. This ensures that the digitally signed document can still be verified as correct in the years after it is created. Swisscom ITSF shall in this process record all relevant information concerning the data issued and received by Swisscom ITSF and shall keep it in safekeeping so that it is available, for the purposes of enabling corresponding evidence to be provided in judicial proceedings, in particular, and ensuring continuity of the trust service.

On the one hand, Swisscom ITSF shall retain the following data for this purpose:

- Log files for the signing process (specifically includes business partner number, process number, process-related data)
- Hash value of the signed document

If Swisscom ITSF itself does not retain the information specified in section 7.2 of these Terms and Conditions of Use, the registration authority shall provide these details to Swisscom ITSF to the extent this is required for purposes of providing the trust service under applicable law. In addition, Swisscom ITSF shall maintain a certificate data base.

Swisscom ITSF shall delete the data described in this section 7.4 after the expiry of a maximum of 39 years from completion of the identity verification process according to section 2.2 of these Terms and Conditions of Use. In the case of identity verification after the request only of advanced electronic signatures in accordance with section 2.2, Swisscom ITSF shall delete this data after the expiry of a maximum of 16 years after completion of the identity verification process.

8 Involvement of third parties

Swisscom ITSF may engage third parties to perform its duties. In particular, Swisscom (Switzerland) Ltd. in Switzerland is used to operate the IT systems for the provision of the trust services. Third parties shall be specifically engaged by Swisscom ITSF to carry out the identity verification process (including retention of the identity verification documentation) (registration authorities).

9 Liability and force majeure

Swisscom ITSF must at all times fulfil the requirements which the law and the technical standards impose on providers of trust services. Swisscom ITSF shall take appropriate state-of-the-art security measures for this purpose. You acknowledge that despite all Swisscom ITSF's efforts, the use of modern technology and security standards, and oversight by an independent agency with regard to compliance with the technical

standards and in the case of qualified electronic signatures oversight by the confirmation body with regard to compliance with the statutory requirements, there can be no guarantee that the trust service will be absolutely secure and free of defects.

Unless Swisscom ITSF can prove that it is not at fault, it shall be fully liable to you for loss or damage incurred by you due to the fact that Swisscom ITSF has not complied with the obligations under the eIDAS regulation.

Unless Swisscom ITSF can prove that it is not at fault, it shall be liable to you for proven damages in the case of other contractual breaches (in particular in connection with advanced certificates and advanced electronic signatures) as follows: Liability for material damage and financial losses due to simple negligence shall be limited to a maximum of EUR 5,000 for the entire contractual term. Swisscom ITSF's liability for indirect loss or damage caused due to simple negligence, consequential losses, lost profit, data losses, loss or damage due to downloads, third party claims, and reputational losses shall be excluded. Swisscom ITSF shall at all times be fully liable to you for personal injury. Swisscom ITSF shall not be liable to you for the proper operation of third party systems, in particular not for the hardware and software used by you or for the subscriber application used by you for controlling the trust service.

Swisscom ITSF shall not under any circumstances be liable to you for loss or damage incurred by you due to the fact that you have either failed to comply with or exceeded a limitation of use. Swisscom ITSF shall likewise not be liable to you if due to force majeure the performance of the service is occasionally interrupted, restricted in whole or in part, or rendered impossible. The term “force majeure” includes in particular natural phenomena of particular intensity (avalanches, flooding, landslides, etc.), acts of war, riots, and unforeseeable official restrictions. If Swisscom ITSF cannot fulfil its contractual obligations, the performance of the Agreement or the deadline for performing the same shall be postponed according to the force majeure event that has occurred. Swisscom ITSF shall not be liable for any loss or damage incurred by Customer because of the delay in the performance of the Agreement.

10 Amendments to the Terms and Conditions of Use

Swisscom ITSF reserves the right to amend and supplement these Terms and Conditions. In particular where amendments are made to the eIDAS Regulation or the Austrian Signature and Confidential Services Act or the regulations issued on the basis thereof, and in the case of orders by the confirmation authority or the supervisory authority or an independent agency for checking advanced electronic signatures, Swisscom ITSF may be forced to adapt both the certificate policy referred to in section 2.1 of these Terms and Conditions of Use and these Terms and Conditions of Use. If any amendments are made, you shall be informed by Swisscom ITSF or by a registration authority delegated by it of the changes at least one month before the date they become effective and the time limit you have for objecting, provided that you have not been registered only for a one-time signature. This information may be sent via SMS to the mobile phone number provided by you or another channel of communication indicated by you. You may refuse to accept the new Terms and Conditions by revoking use of the trust service in accordance with these Terms and Conditions as of their effective date. If you continue to use the trust service after their effective date, this shall be deemed to be acceptance of the amended Terms and Conditions.

11 Applicable law and jurisdiction

If you have your usual place of residence in Austria or are an entrepreneur, all legal relationships in connection with these terms of use are subject to Austrian law.

In the event of any dispute we will endeavour to resolve the dispute amicably. If you are an entrepreneur, the exclusive place of jurisdiction is Vienna, Austria.

12 How to contact us

If you have questions about the services provided in accordance with these Terms and Conditions of Use, you may contact Swisscom ITSF at the following website trustservices.swisscom.com.