Terms and Conditions of Use Swisscom ITSF Trust Service (Qualified and Advanced Electronic Signatures)

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

1 Scope of these Terms and Conditions of Use

These Terms and Conditions of Use shall apply in the relationship between you and Swisscom ITSF IT Services Finance S.E., PKI Dienstleistungen, Mariahilfer Strasse 123/3, 1060 Vienna, Austria, company number 378965b (hereinafter referred to as "Swisscom ITSF") for your use of the Swisscom ITSF trust service with qualified and advanced certificates for qualified and advanced electronic signatures.

2 Services from Swisscom ITSF

2.1 Trust service in general

For your trust services with qualified certificates, 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 these 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

https://www.swisscom.ch/en/business/enterprise/offer/security/digital_certificate_service.html
(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 with real names and certificates with pseudonyms (see sec. 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 qualified 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.

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.

In addition, Swisscom ITSF operates a directory service, which is accessible to the public. The directory service allows to check the identification status of a person so that a person who has already been identified and registered does not have to go through this identification process again. The following data is checked and displayed after the corresponding mobile phone number has been entered: identified for advanced or qualified electronic signature, signature authorisation under CH and/or EU law, confirmed mobile phone number, Swisscom ITSF internal identification serial number and information if the signature authorisation is about to expire (date).

2.3 Issuance of certificate and keys, creation of signature

Swisscom ITSF creates the qualified or advanced certificate and the cryptographic pair of keys for the signing process on a special server (Hardware Security Module, HSM). The qualified or advanced 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. password/SMS authentication process or a permitted App such as the Mobile ID App, 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 qualified or advanced electronic signature for you based on the appropriate certificate.

For each signing process Swisscom ITSF creates a new digital certificate (with a short validity period of 10 minutes) with a new pair of keys.

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

https://www.rtr.at/TKP/was_wir_tun/vertrauensdienste/Signatur/signaturpruefung/Pruefung.en.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 signing service is constantly available, nor shall it be liable for delays or blockages of the network system, availability of mobile services or internet connections. 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. You may find a report on the current availability status of the service here:

https://trustservices.swisscom.com/service-status/

3 Preconditions of use

You have an adequate understanding of digital certificates and of qualified and advanced 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 qualified or advanced 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 connection of the subscriber application to the Swisscom ITSF trust service is the subject of a separate agreement.

You have a means of authentication which is permitted for transmitting declarations of intent for electronic signature (e.g. a mobile phone). Options available for this include password/SMS authentication, an authorised application such as the Mobile ID App or another recognised method of authorising a signature. The actual signature authorisation results from the connection of the subscriber application used by you.

4 Your duties of cooperation

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

When using passwords, to the extent they are required for creating an electronic signature, you undertake not to use any data relating to your personal information (date of birth etc.) for any PIN or password when using the signature approval process. Any records of the PIN or personal password used in connection with authentication must not be disclosed to any other person, must be kept securely and separate from your means of authentication (e.g. mobile phone) or encrypted and must be protected from access by third parties.

If you use a password or a one-time password sent from Swisscom ISTF by SMS as part of the authentication process, you shall ensure that your input of the data requested is always entered on input screens of Swisscom ITSF systems. Further information about this can be found in this document.

If, for example, your mobile device, your SIM card or 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 are additionally obliged to do the following:

- Immediately cease creating signatures,
- If necessary, also change the access data (e.g. on the Mobile ID App or your password) and, if necessary, also block your SIM card.

As soon as there are any changes to a device used for authentication (e.g. your mobile phone number) or changes of your identity data, you shall inform your registration authority or Swisscom ITSF directly of these changes before you sign the next time.

You undertake to take every reasonable and readily available opportunity to protect your device / your mobile phone required 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 a qualified 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 (qualified or advanced electronic signature) for each signature process. Swisscom ITSF has no influence on this choice.

The subscriber application you use will have the advanced or qualified electronic signature linked with a qualified time stamp at Swisscom ITSF.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 within the meaning of Paragraph 886 of the Austrian General Civil Code, so it does not have the same legal effects as a handwritten signature. 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 qualified or advanced electronic signatures created with the Swisscom ITSF Swiss trust service may have different, possibly less extensive effects under the law of a country other than Austria 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 five years, although this period shall be shortened accordingly for qualified electronic signatures if the period of validity of the identification document presented by you expires earlier, or if the identification process selected generally envisages a shorter period.

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. In addition to the applicable laws, the handling of the data shall also be governed by the certificate policy referred to above in section 2.1 of these Terms and Conditions of Use.

Swisscom ITSF shall involve Swisscom (Switzerland) Ltd, based in Switzerland, in the provision of trust services. Swisscom (Switzerland) Ltd operates the IT systems for the provision of trust services and these IT systems are located in Switzerland. The advanced or qualified certificates are thus issued on servers in Switzerland. In this regard the data processing in Switzerland is done by Swisscom (Switzerland) Inc on behalf of Swisscom ITSF. Swisscom ITSF has concluded the necessary data protection agreements with Swisscom (Schweiz) AG.

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

7.2 Identity verification documentation

For the purpose of creating the digital certificate and to maintain the verifiability of the trust service, Swisscom ITSF or the registration authority commissioned by Swisscom ITSF 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):

In-person identification:

- 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) unless you have proven your identity by an identity provider or information from an identification verification procedure about a prior identification check using a photo ID can be presented.
- Information contained in the identity document (in particular: first names, last name, date of birth, gender, validity date and serial number of identity document, nationality)
- Personal means of authentication used (e.g. mobile phone number)
- A photograph of you taken during the identification meeting.

Video identication or auto-video identification

- A photograph of you taken during the video identification
- Photographs of the relevant pages of the identity document produced by you
- Audio recording of the video meeting
- Technical details (e.g. IP address) of the device used by you
- Information contained in the identity document (in particular: first names, last name, date of birth, gender, validity date and serial number of identity document, nationality)
- Personal means of authentication used (e.g. mobile phone number)
- If supported: Data downloaded from the chip of your identity document (e.g.: first names, last name, date of birth, validity date and serial number of identity document, nationality)

eID

- Personal means of authentication used (e.g. mobile phone number)
- Data downloaded from the chip of your identity document (e.g.: first names, last name, date of birth, validity date and serial number of identity document, nationality)

Identification based on your e-Banking Account

- Information transmitted by you or the operator of the signature application (in particular: first names, last name, date of birth, validity date and serial number of identity document, nationality)
- Bank account used for eBanking (IBAN/BIC/name of bank)
- Personal means of authentication used (e.g. mobile phone number)
- Schufa ID or ID of another credit information company
- Data on reference transaction
    - Account holder
    - Account number
    - Time of reference transfer
    - Transaction authorisation procedure
- Other information and documents in the certificate provided by you for example in respect of your organisation, such as Commercial Register extracts, email address, powers of attorney. Articles of Association/partnership agreements or other documentary evidence concerning specific attributes)

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 a qualified or advanced certificate, which may contain the following information concerning you:

If the subscriber application envisages the use of real names:

- First names, last name
- Informal name for simplification purposes (e.g. first name)
- Two-digit ISO 3166 country code

If the subscriber application envisages the use of a pseudonym:

- Pseudonym
- Informal reference for ease of display (e.g. reference PSEUDONYM)
- Two-digit ISO 3166 country code

In addition, the certificate may also contain the following details:

- Additional information e.g. to ensure the uniqueness of the digital certificate:
- Name of company
- Number/ID of the identity document presented
- Mobile phone number
- Text displayed by the signature application used by you for authorising your signature (e.g.: “Please confirm the signature in the file test.pdf in Application XYZ”)
- 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

Swisscom ITSF’s registration authority 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 (possibly with the assistance of a 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 the last signing process. 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 7 years from the last signing process. 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.

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 the Terms and Conditions of Use, then Swisscom ITSF's registration authority shall supply these details to the extent this is required for purposes of providing the trust service in line with applicable law. Swisscom ITSEF shall manage a certificate data base.

Swisscom ITSF shall delete the data described in this section 7.4 after the expiry of a maximum of 36 years from completion of the identity verification process according to section 6 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 13 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 (Schweiz) AG in Switzerland will be engaged to operate the IT systems for the provision of the trust services and Swisscom Trust Services AG will be engaged as the registration authority and contact for all questions relating to this service, and as the supplier of technology and services. Further third parties shall be specifically engaged by Swisscom ITSF to carry out the identity verification process (including retention of the identity verification documentation) (further 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,
- 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 proves that it is not at fault, it shall be liable to you without limitation for any loss or damage suffered by you because Swisscom ITSF culpably failed to comply with its obligations under the eIDAS Regulation. If Swisscom ITSF informs you directly or through the operator of the subscriber application before a signature is created of a transaction limit for transactions involving monetary payments in connection with the creation of an electronic signature using the Swisscom ITSF trust service and if that transaction limit is apparent to third parties, e.g. due to the fact that the transaction limit is displayed in the certificate, Swisscom ITSF shall not be liable for any losses caused by use of the services in excess of these limits.

Unless Swisscom ITSF can prove that it is not at fault, in the event of other breaches of contract (in particular in connection with advanced certificates and advanced electronic signatures) Swisscom ITSF shall be liable to you for the proven losses as follows:

Liability for material damage and financial losses due to simple negligence shall be limited to a maximum of CHF 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, unforeseeable official restrictions and pandemics or epidemics. 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 only been registered for a one-time signature. This information may be sent via SMS or another mode of communication indicated by Swisscom ITSF to the mobile phone number provided by you.

These amendments shall be deemed accepted by you if you have not raised any objections to the amendments within the period for objections; you will be informed of the amendments and of your right to object and of the period for objections. You may also 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

All legal relationships in connection with these terms of use and all entrepreneurs are subject to Austrian law. Otherwise, the law of the country in which you are usually resident shall apply if it is a country to which the eIDAS Regulation applies or you are usual resident of Switzerland. Subject to mandatory jurisdictions, for all disputes arising from or in connection with these Terms of Use Vienna, Austria is the exclusive place of jurisdiction.

In the event of any dispute we will endeavour to resolve the dispute amicably.

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:

https://trustservices.swisscom.com/en/