Terms and Conditions of Use for the use of the Swisscom certification service with digital certificates for advanced and regulated electronic seals for organisations (Swisscom 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 the customer (organisations with a corporate identification number such as legal persons or administrative entities, hereinafter "Seal Creators") and Swisscom (Switzerland) AG, Alte Tiefenaustrasse 6, Worblaufen, Switzerland, company ID CHE-101.654.423 (hereinafter "Swisscom") for the use of the Swisscom certification service with digital certificates for advanced and regulated electronic seals.

2 Swisscom's Services

2.1 Certification service in general

For your certification services with regulated and qualified certificates, Swisscom is an accredited certification services provider in Switzerland pursuant to the Swiss Federal Act concerning certification services in the area of electronic signature (Electronic Signature Act, ZertES; SR 943.03) and is audited and supervised by the ZertES accreditation authority. Swisscom provides its certification services with certificates for advanced electronic seals in accordance with internationally recognised technical standards.

The certification service is provided in accordance with the Swisscom certificate policy in its then current version. This certificate policy – Certificate Policy (CP/CPS) for the issuance of "Diamant" (Diamond) class certificates (regulated) and "Saphir" (Sapphire) class certificates (advanced) – forms an integral part of these Terms and Conditions of Use. The documented may be viewed and downloaded online at https://trustservices.swisscom.com/repository (in the "CH" section).

As part of the certification service, Swisscom creates a digital certificate which includes information about the Seal Creator. Swisscom links this certificate with the file to which the Seal Creator, acting through its employees or other representatives, wishes to affix an electronic seal (e.g. invoice in PDF format). This enables the digital electronic seal on the document to be assigned to the Seal Creator. The result is that third parties can also rely on the digital electronic seal and on the information contained in the certificate.

In each case, depending on the order in the application form, a regulated electronic seal pursuant to Article 2 letter d ZertES or an advanced electronic seal is created. No other type of use of the digital certificate is permitted in connection with the use of the certification service in accordance with these Terms and Conditions of Use ("limitation of use").

2.2 Identity verification process and retention of the information

Within the identity verification process, Swisscom or the registration authority appointed by Swisscom examines the information concerning the Seal Creator and the identity of its representatives (e.g. employees, if the Seal Creator is not a natural person itself) with reference to documents and information requested from the Seal Creator by Swisscom or the registration authority appointed by Swisscom (customer data). The examination of customer data may occur in different ways and upon presentation of various documents (e.g. identity card, commercial register extract, extract from the UID register) and is determined in accordance with the specific structure of the identity verification process by Swisscom or the registration authority appointed by it.

Swisscom registers and files the customer data collected in the identity verification process in accordance with the applicable regulations. The handling of customer data is described in section 7 of these Terms and Conditions of Use.

2.3 Issuance of certificate and keys, seal creation

Swisscom creates the digital certificate and the cryptographic pair of keys for the seal creation process on a special server in a secure signature creation unit (Hardware Security Module). The digital certificate is a certificate which assigns to the Seal Creator the public key of the asymmetrical cryptographic pair of keys. The Seal Creator alone has the ability, through its SSL/TLS protected access, to have electronic seals created in this manner (see also in this regard sections 3 and 4 of these Terms and Conditions of Use).

The digital certificate has a maximum validity period of 3 years.

2.4 Verification of the digital electronic seal

The Swisscom certification service allows the validity of the electronic seal to be validated. Third parties also (often referred to as the "relying party") can validate the validity of the electronic seal, e.g. for regulated seals by using the validator provided by the federal government on the website https://www.validator.ch. The information provided in section 5 of these Terms and Conditions of Use must be noted concerning the legal effects of the electronic seal.

2.5 Availability

Swisscom shall endeavour to provide the certification service continuously. Swisscom shall not, however, be liable for ensuring that the signing service is constantly available. Swisscom 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 shall endeavour in this process to take account of the interests of the users of the certification service.

3 Preconditions of use

The Seal Creator has an adequate understanding of digital certificates and electronic seals.

The Seal Creator uses access certificates to authenticate an application (hereinafter "subscriber application") with Swisscom, which it operates itself or has a third party operate, and which enables the Swisscom certification service to be used. The subscriber application may for example be the accounting software of the Seal Creator or the internet portal of a third party. The party that operates the subscription application and ensures its connection to the Swisscom certification service is referred to as the subscriber. The linking of the subscriber application to the Swisscom certification service is the subject of a separate agreement with the subscriber (hereinafter "All-in Signing Service Agreement"): If the Seal Creator itself is also the subscriber, it concludes an All-in Signing Service Agreement itself. If the Seal Creator is not itself the subscriber, the use of the certification service in accordance with these Terms and Conditions of Use is conditional on the one hand on the existence of an All-in Signing Service Agreement concluded by the subscriber and on the other hand on the authorisation of the subscriber by the Seal Creator to the linking of the subscriber application.

The terms and conditions of the subscriber application used by the Seal Creator may result in limitations on the use of the certification service.

4 Cooperation obligations of the Seal Creator

The Seal Creator shall provide Swisscom with the application form, completed by the Seal Creator and signed by hand or by qualified electronic signature, for the issuance of a certificate. In it the Seal Creator also confirms its acceptance of these Terms and Conditions of Use.

If the Seal Creator and the subscriber are identical, it shall also provide Swisscom with the configuration and acceptance declaration. If the Seal Creator is not itself the subscriber, the configuration and acceptance declaration shall be completed, signed and provided to Swisscom by the subscriber.

The Seal Creator must authenticate the subscriber application with Swisscom:

- If the Seal Creator and the subscriber are identical and advanced electronic seals are to be created, the Seal Creator shall submit the access certificate to Swisscom electronically (e.g. by email).
- If the Seal Creator and the subscriber are not identical, the Seal Creator shall authorise the subscriber with Swisscom by a declaration to that effect in the application form. The Seal Creator thereby also acknowledges and agrees that the access certificate may be used by Swisscom with the subscriber application of the subscriber.
- If regulated electronic seals are to be issued, the Seal Creator shall create the private key to the access certificate on an HSM (minimum standard FIPS 140 level 2) or other by Swisscom authorized storage solution and shall thereafter deliver the access certificate. In case a technical process for the creation of access certificates is not authorized by Swisscom the creation will happen in a joint ceremony with Swisscom's registration authority. The Seal Creator must then ensure on an ongoing basis that the HSM can be reached by the subscriber application using the private key.

As soon as the subscriber application has been linked to the Swisscom certification service by means of access certificates, there is no further individual authentication for each seal creation process, i.e. all hashes transferred through this interface are marked – depending upon the order in the application form – with an advanced or a regulated electronic seal. The Seal Creator therefore ensures that the persons that it allows to access the certification service through the subscriber application in accordance with these Terms and Conditions of Use are first made aware of the following points:

- the manner of operation of the certification service,
- the preconditions of use according to section 3,
- the cooperation obligations according to section 4,
- the legal effects according to section 5.

In any case, the Seal Creator shall be liable for the conduct of such persons in relation to the use of the certification service in accordance with these Terms and Conditions of Use in the same manner as if it were its own.

The Seal Creator undertakes that, as part of the identity verification process, both it and its representatives will provide Swisscom and/or the registration authority with complete and true information.

Records, if any, of the password for retention of the private key or the private key of the access certificate for authentication with the servers of the Swisscom certification service may not be disclosed to any unauthorised persons, must be securely stored and must be protected against unauthorised third party access.

The Seal Creator undertakes to have the digital certificate issued to it declared invalid immediately if its password has been disclosed to any unauthorised persons, the private key of the access certificate has been compromised or the Seal Creator knows or suspects that an unauthorised person has become aware of the password for retention of the private key or of the private key (compromising). Instructions for the declara-

tion of invalidity may be given to the registration authority or Swisscom in accordance with the procedures set forth in the certificate policy.

The Seal Creator undertakes to inform Swisscom immediately of any changes to its name or, respectively, company name and never to use certificates containing incorrect customer data within the meaning of section 2.2 of these Terms and Conditions of Use.

The Seal Creator undertakes to take every reasonable and readily available opportunity to protect its infrastructure linked to the Swisscom certification service from attacks and malware ("viruses", "worms", "Trojan horses" and the like), particularly through using software that is continually updated.

The Seal Creator undertakes to check the electronic seals after they have been created in accordance with section2.4 of these Terms and Conditions of Use and to promptly report any discrepancies in the digital certificate to Swisscom.

5 Legal effects of the electronic seal

The certification service in accordance with these Terms and Conditions of Use creates advanced or regulated electronic seals and links them to a qualified electronic time stamp.

The use of the electronic seal is intended as a rule to guarantee proof of origin and the integrity of the content of a file. The electronic seal is not to be confused with the legal concept of the electronic signature. Furthermore, the legal effects of the higher-order regulated electronic seal are not the same as those of the advanced electronic seal. It is the Seal Creator's responsibility to clarify in advance the legal effects of the type of electronic seal chosen (with and without time stamp), if necessary in consultation with the subscriber. Swisscom disclaims any responsibility in this regard.

Regulated electronic seal: The regulated seal created using the Swisscom certification service meets the definition set forth in Article 2 letter d of the Swiss Electronic Signature Act (ZertES; SR 943.03) and is based on a regulated certificate (Swisscom "Diamant" certificate class) issued to the Seal Creator.

Advanced electronic seal (certificate from Swisscom "Saphir" class): The advanced electronic seal created using the Swisscom certification service has the characteristics defined in the CP/CPS.

Qualified electronic time stamp: The qualified electronic time stamp created using the Swisscom certification service meets the definition set forth in Article 2 letter j ZertES.

Neither the advanced electronic seal nor the regulated electronic seal has the same legal effects as a handwritten signature or a qualified electronic signature. Depending on the particular situation, certain documents thus require a handwritten signature, a qualified electronic signature or a regulated electronic seal, as the case may be with an electronic time stamp, in order to be legally effective.

The Seal Creator acknowledges that it may incur liability towards third parties pursuant to Article 59a of the Swiss Code of Obligations for any damages suffered by them due to their reliance on a valid regulated certificate of Swisscom.

The Seal Creator further acknowledges that the digital electronic seals created with the Swisscom certification service may have different, possibly less extensive effects under the law of a country other than Switzerland and that legal requirements might not be met.

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

6 Duration

The Seal Creator may use the certification service in accordance with these Terms and Conditions of Use for the duration of the All-in Signing Service Agreement with Swisscom, provided that a valid certificate is in place, the information contained therein has not changed and the Seal Creator complies with these Terms and Conditions of Use.

7 Handling data of the Seal Creator

7.1 General

Swisscom collects, stores and processes only data which is needed to provide the certification service. Handling of the data shall be governed not only by the applicable Swiss data protection law but also by the certificate policy referred to in section 2.1.

In accepting the Terms and Conditions of Use, the Seal Creator expressly accepts the recording and processing of the customer data collected from it as described in this section.

7.2 Identity verification documentation

For the purpose of creating the digital certificate, of maintaining the verifiability of the certification service and for any revocation of certificates, Swisscom collects and stores the following data:

- Information and documents provided by the applicant in the identity verification process in accordance with section 2.2 of these Terms and Conditions of Use, e.g. certified commercial register extract, extract from the UID register, powers of attorney and other documentation concerning specific attributes.
- Mobile telephone number of the applicant for authentication in the event of any revocation.
- If the Seal Creator is not a natural person, from the representative of the Seal Creator that submits the application to Swisscom for the issuance of the digital certificate: A copy of the relevant pages of the identity document (passport, identity card) with the information contained therein (in particular, gender, first names, last name, date of birth, valid date of identity card, nationality).

7.3 Digital certificate

Based on the data which has been provided by the Seal Creator and collected in the identity verification process, Swisscom shall issue a digital certificate containing the following information concerning the Seal Creator:

- Formal name or company name (according to evidence relating to the organisation)
- Company identification number or, for advanced seals, also other registration numbers
- Two-digit ISO 3166 country code
- Time of issuance of the certificate, time of creation of the seal

After completion of the seal creation process, the digital certificate is included in the file that was marked with a digital electronic seal. Anyone in possession of this file may view the aforementioned information from the certificate at any time. This enables third parties to review information concerning the Seal Creator and to also see that Swisscom as an accredited Swiss certification service provider guarantees the certification of this data and the seal creation process.

7.4 Data after completion of the seal creation process

Swisscom 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 the Seal Creator to use the certification service. Further, Swisscom shall retain various data concerning the identity verification process, the digital certificate and the seal creation process for a period of 7 years (advanced) or 11 years (regulated) from the last seal creation process. This ensures that the document marked with an electronic seal can still be verified as correct in the years after it is created. Swisscom shall in this process record all relevant information concerning the data issued and received by Swisscom 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 certification service.

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

- Log files for the seal creation process (specifically includes access identification, process number, process-related data)
- The hash value of the document to which an electronic seal was applied

On the other hand, Swisscom shall retain the information specified in section 7.2 of the Terms and Conditions of Use and shall manage a certificate data base.

Swisscom shall delete the data described in this section 7.4 after a maximum of 7 years (advanced) or 11 years (regulated) after the expiry of the digital certificate.

In the event of the cessation of the business operations of an external registration authority, the data stored there shall be transferred to Swisscom.

8 Involvement of third parties by Swisscom

Swisscom may engage third parties to perform its duties. Third parties shall be specifically engaged to carry out the identity verification process and also to store Swisscom data processed by third parties (registration authorities).

9 Liability and force majeure

Swisscom must at all times fulfil the requirements which the law and the technical standards impose on providers of certification services. Swisscom shall take appropriate state-of-the-art security measures for this purpose. The Seal Creator acknowledges that despite all Swisscom's efforts, the use of modern technology and security standards, and oversight by the ZertES accreditation authority with regard to compliance with the statutory requirements for regulated electronic seals, there can be no guarantee that the certification service will be absolutely secure and free of defects.

Unless Swisscom can prove that it is not at fault, it shall be fully liable to the Seal Creator in relation to regulated certificates and electronic seals based upon them for any losses or damages incurred by the Seal Creator due to the fact that Swisscom has not complied with the obligations under the ZertES.

Unless Swisscom can prove that it is not at fault, it shall be liable to the Seal Creator for proven damages in the case of other contractual breaches as follows:

If the Seal Creator and the subscriber are identical and the subscriber has concluded an All-in Signing Service Agreement directly with Swisscom, liability shall be determined in accordance with the terms of this All-in Signing Service Agreement.

For all other scenarios (e.g. the Seal Creator and the subscriber are not identical, or the All-in Signing Service Agreement of the subscriber was not concluded with Swisscom, but with a partner of Swisscom) the following shall apply:

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'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 shall at all times be fully liable to the Seal Creator for personal injury. Swisscom shall not be liable to the Seal Creator for the proper operation of third party systems, in particular not for the hardware and software used by the Seal Creator or for the subscriber application used by the Seal Creator for controlling the certification service.

Swisscom shall not under any circumstances be liable to the Seal Creator for loss or damage incurred by the Seal Creator due to the fact that it has either failed to comply with or exceeded a limitation of use. Swisscom shall likewise not be liable to the Seal Creator 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 cannot fulfil its contractual obligations, contractual performance or the deadline for contractual performance shall be postponed according to the force majeure event that has occurred. Swisscom shall not be liable for any loss or damage incurred by the Seal Creator because of the delay in contractual performance.

10 Amendments to the Terms and Conditions of Use

Swisscom reserves the right to amend and supplement these Terms and Conditions. In particular where amendments are made to ZertES and its implementing legislation, and in the case of orders by the ZertES accreditation authority, Swisscom 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, the Seal Creator shall be informed by Swisscom 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 it has for objecting.

This information may be sent by SMS to the mobile telephone number provided by the Seal Creator or by email. The Seal Creator may refuse to accept the new terms and conditions by refraining from using the trust service in accordance with these Terms and Conditions of Use from the time they take effect. If the Seal Creator continues to use the trust service after they have taken effect, this shall be construed as acceptance of the amended terms and conditions.

11 Applicable law and jurisdiction

All legal relationships in connection with these Terms and Conditions of Use shall be subject to Swiss law.

In the event of any dispute the parties shall endeavour to resolve the dispute amicably. Jurisdiction shall lie in Bern, Switzerland, unless required otherwise by law.

12 How to contact us

If there are any questions about the services provided in accordance with these Terms and Conditions of Use, the Seal Creator may contact Swisscom at the following website https://trustservices.swisscom.com .