SignatureNet

General Terms and Conditions of Business of GSN Global Signature Net AG («SignatureNet») for Data Storage for Issuing Banks («GTCs issuing banks»)

1 Coverage

These «GTCs for issuing banks» establish the general conditions for operation of the SignatureNet server, the delivery and publication of signature data, the areas of information security, and the secure issuance of logon-IDs and passwords.

2 Definitions

Administrator: For SignatureNet, a bank administrator is the person at the bank who can change bank master data, register authorized users, or view statistics. The bank administrator is specfically designated in the contracts by the issuing and/or user bank. The bank can designate several administrators with different rights.

Authorized users: Authorized users are those persons who were registered by their bank administrator in SignatureNet as administrators or users.

Issuing bank: The issuing bank stores its own signature directory on the SignatureNet server and makes it available to user banks (correspondent banks) through a secure https-Internet connection. The issuing bank determines which user bank may view its signatures and which may not.

SignatureNet server: The SignatureNet server is a computer that stores the data (bank master data, authorizations, signature data, etc.) of the issuing and user banks, and permits secure and authorized Internet access.

User bank: If authorized by the issuing bank, the user bank can view the signature directories of the issuing banks over the Internet with a browser and can make a visual signature comparison.

3 SignatureNet's performance

3.1 Data retention

SignatureNet operates the SignatureNet server as a central database with which all connected issuing banks and user banks can store or view signature directories to the extent defined for them. SignatureNet thereby ensures that the security level customary for banks for such applications is maintained during operation. The signatures of the issuing banks are stored as provided by the issuing bank. Sensitive data, such as individual signatures, or passwords, are stored encrypted in the database. Maintenance of content (updating, completeness, correctness) of the data provided by the issuing banks is not part of the contractual performance of SignatureNet.

3.2 Availability

The SignatureNet server is in operation 7 x 24 hours, with a reaction time – the time from reporting of a problem to the start of malfunction repair – of 30 minutes during the regular business hours of SignatureNet. These hours are Mondays – Fridays from 8:00 a.m. - 5:00 p.m. (CET), except for legal holidays at SignatureNet's registered office. Outside these business hours, reaction time is 4 hours. SignatureNet endeavors to ensure operation as free from interruption as possible, but it is not able to provide an availability guarantee. Malfunctions are repaired within an appropriate amount of time, whereby SignatureNet, in case of a total breakdown of the SignatureNet server, will, if possible, continue repair work without interruption until operational readiness is restored. SignatureNet will perform planned maintenance work on the SignatureNet server only outside its normal operating hours.

The hardware and operating system software used for the SignatureNet server correspond to the generally recognized technological state of the art and are updated continually. The SignatureNet server is constantly monitored during operation.

3.3 Statistics and monitoring functions of the issuing bank's administrator

For security reasons, all access to the signatures and authorizations and all actions performed are recorded without gaps. This permits the administrator to determine at all times which User Bank has seen which signature. Corresponding statistics are made available to the administrator. These include user lists, login statistics and audit trails, for example. The corresponding data is stored by SignatureNet with the regular backup and is available to the administrator for online access at no cost for 3 years from the date of initial storage. Access to stored data older than 3 years is subject to charge. The total storage period is 10 years.

3.4 Security

a) **Security standards**
The security parameters needed for the operation of SignatureNet are established by SignatureNet. The web application is subjected to a vulnerability scan at least once a year by an independent, external IT security company. In addition the issuing bank has the right to check the security concept and the systems of SignatureNet (audit). This includes in particular the right to perform a penetration test at the issuing bank's own expense, or to have such a test performed by a specialist firm. SignatureNet must be notified of such tests at least 4 weeks in advance.

b) **Physical security**
The servers used are located in locked cabinets in a specialized computer center. The center has the customary safety measures, such as fire protection, monitoring and entry control.

c) **Firewall**
The firewall systems employed by SignatureNet correspond to the technological state of the art in both hardware and software. The administration and configuration of the firewalls are subject to a restrictive process. Changes in the control set can only be carried out by SignatureNet as system owner. Regular monitoring (once per year) by the external banking security specialist team guarantees compliance with the security concept.

d) **Virus protection**
In order to provide the greatest possible protection against viruses and malicious code, the servers are scanned several times each day. In addition, the virus scanner used is updated daily.

e) **Data transfer**
All data from the issuing bank's client to the SignatureNet server and from the SignatureNet server to the user bank's client is transmitted encrypted with SSL (minimum 128 bits) over a secure https connection.

f) **Backup**
A backup, which is run daily guarantees that the current database can be restored at any time.

g) **Access protection**
Access authorizations for the administrators of issuing and user banks are granted by SignatureNet as soon as the request is verified and the contracts for issuing or user banks are signed. For security reasons, this access authorization is sent as follows: logon-ID (hereafter «ID»") by email, password for the administrator by fax or SMS and registered letter together with the signed contracts for issuing or user banks, and the applicable GTCs by post. SignatureNet assigns only one access authorization for each bank. Additional internal administrators or users can be recorded by this administrator online.ID and password are always mandatory for online access to the SignatureNet server. As a third identification element, the IP address of the PC that is logging in is compared to the IP range reported by the issuing or user bank and verified by SignatureNet. If the bank uses dynamic IP addresses, the third identification

element consists of an access code for one-time login, which is generated by SignatureNet and sent by email to the user's personal business email address.
Access is blocked if an incorrect entry is made five times. Each access is recorded. It is mandatory that the passwords for the administrators as well as the authorized users must comply with guidelines published by SignatureNet and must be changed periodically.

h) Depositing of software (escrow agreement)

To ensure that the issuing banks as customers of SignatureNet are in a position to perform the necessary maintenance work or continue the service themselves or through third parties if

- SignatureNet relinquishes its business (except for a liquidation due to takeover by another company with all rights and duties)
- SignatureNet enters into judicial estate proceedings or the same is requested from the responsible bankruptcy authority
- SignatureNet enters bankruptcy
- in the event of an infringement of contractual duties by SignatureNet that is verified in writing, and which massively impairs SignatureNet's ability to function or makes such functioning impossible,

all data and information needed to accomplish this (particularly the software's source code, the system description, the functional description, the admin accounts and the admin passwords) are deposited for each new release, version, etc., but at least once per year, in the bank safe of a major Swiss bank..
Each issuing bank shall have the right to be recorded on a list of beneficiaries. Each issuing bank may request via SignatureNet that it be listed accordingly on the list of beneficiaries. Such inclusion on the list shall be undertaken at no charge for the issuing bank. The issuing banks shall also have the right to engage an escrow agent to form an escrow agreement with SignatureNet.

3.5 Help desk

Online help is available to authorized users of SignatureNet to assist them with questions about operation, etc. The SignatureNet help desk can also be reached by email or phone.

4 Duties of assistance of the issuing bank

4.1 Master data

The issuing bank must completely and correctly fill out the master data required by SignatureNet in the contract for issuing banks. If there are changes, the issuing bank must immediately update the master data stored on the web application www.signaturenet.org.

4.2 Delivery of signatures

A prerequisite for publishing signatures in SignatureNet is that the signatures of the issuing bank be available in electronic form.
The initial recording of data is made by SignatureNet (subject to charge) or by the bank itself online. Modifications, deletions or additions of signatories can be made by the bank itself online via a secure https connection. In addition, the issuing bank can always produce a standard PDF from their data.
Banks that already store their data in a database must convert the data into the format required by SignatureNet, or must have such data converted by SignatureNet for a fee.

4.3 Updating

The issuing bank is responsible for maintaining and updating its own data on the SignatureNet server. An administrator with the right to make changes (Maker) may transfer the personal data, signatures, signature rules, etc. online on the SignatureNet server for this purpose. All changes must be checked and approved by a second person (dual-control principle, Checker). SignatureNet agrees to clearly display the date and time of the display on every signature page. The display shall also include the name of the user as well as the date on which the data record was most recently changed.The issuing bank is obligated to update its data at least once a year.

4.4 Signature rules

The issuing bank is responsible for publishing its specific signature rules on the SignatureNet server. Sufficient space is made available for this purpose on the signature pages. SignatureNet makes no guarantee for the correctness, completeness, and current status of information and messages that the issuing banks publish on the SignatureNet Internet pages made available to it. In particular, SignatureNet makes no guarantee for the names, titles and signatures contained therein nor for the signature rules.

4.5 Authorization of user banks

Each issuing bank determines which user bank may view its directory. The administrator of the issuing bank can authorize user banks online by clicking on the corresponding check box of the desired bank in a list. The database contains the names of all banks worldwide and is equipped with corresponding search functions. It is classified by countries and regions. It is also possible, for example, to authorize or block all banks of a country or region in general. As soon as the issuing bank authorizes a user bank, the corresponding authorizations are automatically granted on the SignatureNet server, if the user bank has signed the contract for user banks. The administrator can block an authorization online at any time by deselecting the corresponding check box.
SignatureNet provides an automated email tool that passes on to the issuing bank requests of user banks to be authorized.

4.6 Registration of the issuing bank's employees as authorized users

The issuing bank's administrator can register its bank-internal employees as additional administrators or users (summarized as «authorized users»") online. He or she must provide various details on the new user's person. The number of authorized users is unlimited.
These details are sent encrypted with SSL (at least 128-bit) over a secure https connection to the SignatureNet server and stored in the database. The authorized users must change the password upon first login, and thereafter at regular intervals.
The issuing banks are responsible for ensuring that their authorized users comply with the security regulations contained in the «GTCs for issuing banks».

4.7 Security

4.7.1 Authorization controls

SignatureNet employs the following authorization controls for use of the data provided by the issuing bank:
Each authorized user of a user bank that has a valid contract for user banks must log on to SignatureNet with the ID and password issued by his or her bank's administrator. After this information has been verified, a check is made whether the authorized user has logged on from a PC belonging to the IP range used by the user bank. Authorized users at banks with dynamic IP addresses must also enter an access code for one-time login.This measure ensures that the authorized user can only log on from his or her workplace.
Once this information is checked by SignatureNet and the user bank accepts the conditions of use, the user bank (exclusively) is shown those issuing banks whose signature directories it is permitted to see.

These conditions of use essentially are:

- that the information and signatures may be used only for the purpose of visual signature checking
- that the signatures or the PDF may not be stored permanently on the computer
- that paper copies of the signatures and other information may not be made, nor may they be permanently (i.e. outside the cache memory) stored electronically (screen shots print screen etc.). Excepted from this are copies on paper for the purpose of visual verification or documentation of a signature check performed in a specific case
- that the authorized user must ensure that the information and signatures are not made available to third parties, except for audit purposes or to comply with statutory requirements

- that the authorized user accepts that all his or her actions will be recorded and stored through monitoring
- that ID and passwords are personal and secret and must be kept secure and separate from each other. Under no circumstances may they be passed on or revealed to other persons
- that the signature must be retrieved each time or the PDF file downloaded anew, and that the display date must be noticed.

The type of provision of signature data determines what the user bank can do. The authorized users of the user bank can view only individual signatures in the browser.

4.7.2 Proof of identity

Each authorized user who proves his or her identity with ID and proper password (self-identification) from a PC within the IP range reported by the issuing bank and verified by SignatureNet is considered by SignatureNet as an authorized person. This applies regardless of whether this person is in fact authorized to have access. Accordingly, each person who correctly identifies himself or herself has access to the corresponding business relationship. All activities that are based on a correct identification check by the system are the responsibility of the issuing bank involved and are legally binding for it.

4.7.3 Authorized users of banks with dynamic IP addresses must also enter a one-time code.Duties of care

The issuing bank and/or authorized user are required to exercise special caution in storing the IDs and passwords that are provided for proof of identity.

IDs, passwords, and the like are personal, must be kept secret, and must be stored securely and separate from each other. Under no circumstances may they be passed on or revealed to other persons.

If there is reason to assume that another person knows the ID or password, the issuing bank and/or authorized user must change, delete, or block the ID or password immediately. The loss of ID and password shall be reported to SignatureNet without delay.

The issuing bank is responsible for ensuring that its administrators, any sub-administrators and authorized users who are given IDs and passwords observe these obligations.

4.7.4 Risks

The issuing bank is aware of the risks resulting from the movement of SignatureNet Internet traffic over open facilities that are generally accessible (such as public and private data provision networks, Internet servers, access providers). On the SignatureNet Internet page, the data to be transferred is encrypted, except for the sender and recipient. But with the encryption, targeted manipulations of the issuing bank's IT system by unauthorized persons – in particular via Internet – cannot be prevented. SignatureNet is not liable for these manipulations. In order to combat errors and abuses, if a connection is made with SignatureNet over the SignatureNet Internet page, the issuing bank promises to monitor the correctness of the selected SignatureNet address as well as the encryption of the data transfer by means of the security reference. In the event of any irregularity, the connection will be terminated immediately and the findings reported to SignatureNet.

It is possible that an unauthorized third party will attempt to gain access to the issuing bank's IT system unnoticed while SignatureNet is being used. Accordingly, the issuing bank should take the normal protective measures to minimize the security risks that exist on the Internet (such as use of up-to-date anti-virus programs and firewalls). It is the responsibility of the issuing bank to keep fully informed about the required safety precautions. In addition, the issuing bank is obligated to take the necessary safety precautions to secure any data stored on its IT system.

4.7.5 Block

Each issuing bank can limit access to the SignatureNet Services itself by blocking or deleting individual authorised users or by blocking its own signatures.

4.7.6 Country-specific barriers

The offering of services to customers is subject in part to country-specific legal restrictions. If SignatureNet does not have the required local authorizations in the country involved, the range of services of SignatureNet for those authorized accesses in that country must be restricted on a country-specific basis. These restrictions are subject to ongoing changes in the laws of each individual country and in the international community as a whole..

The issuing bank takes note of this and accepts that SignatureNet is entitled to adjust or restrict the range of services offered on a country-by-country basis – regardless of an authorization reference agreed on individually and without separate advance notice. SignatureNet is obligated to inform the issuing banks of a country-specific restriction as soon as possible, however, although not later than with the corresponding implementation.

4.8 Defense against third-party claims

The issuing bank will defend, at its own cost, any claims of third parties that result mainly from the use of the data provided by it to the SignatureNet server and without contributory negligence by SignatureNet, and will indemnify SignatureNet as long as the issuing bank is informed of this as soon as possible, granted control of the legal process or the out-of-court settlement of the lawsuit, and quickly provided all correspondence in the matter and other necessary documents.

5 Stipulations of use

The stipulations of use for the authorized user of SignatureNet are based on the contract for user banks, which is to be separately signed.

6 Fees

6.1 Fees for the user bank

SignatureNet is free of charge for user banks.

6.2 Fees for the issuing bank

The annual recurring fees for the issuing bank are based on the offer, and do not include value added tax and/or similar withholding tax or other governmental levies. The fee periods are based on the calendar year.

The fees are billed annually in January and are due within 30 days.

6.3 Contract termination during the calendar year

If the issuing bank terminates the contract, the fees already paid will expire (exception see item 8). If notice of termination arrives at SignatureNet after November 30, the issuing bank remains obligated to pay the fees for the following calendar year. If SignatureNet terminates the contract, it returns at most the issuing bank's already paid fees on a pro rata basis.

7 Liability

Subject to the stipulations of item 4.8 and further mandatory legal liability for gross negligence and willful misconduct, no contract partner is liable under this contract.

8 Changes to the contract

The issuing bank understands that SignatureNet can change the «GTCs for issuing banks» and the «GTCs for user banks» at any time.

If the change significantly impairs or restricts the use of SignatureNet by the issuing bank, then the issuing bank will be notified of this fact two (2) months in advance by means of registered letter. This would be the case, for example, if SignatureNet were to change the fees, security, or the rights and duties of the issuing bank.

Minor changes (e.g. typographical errors or changes of address, etc.) shall be considered legally binding for the issuing bank when appropriate notice is given. Two months' notice shall be given except in urgent cases. If the issuing bank does not accept the change, it must stop using the information / services involved or cancel the contract within 4 weeks of announcement. Already paid fees will be returned on a pro rata basis only in exceptional cases for significant changes.

9 Data protection

The issuing bank is responsible for the legal procurement of the data stored on the SignatureNet server. The issuing bank, as editor of the corresponding data, is solely responsible for data maintenance. In particular, it bears responsibility for compliance with the applicable data protection stipulations in cross-border data traffic. SignatureNet is not responsible for the user bank's compliance with the stipulations of use or for the compliance of the issuing or user bank with data protection regulations.

10 Duration and termination

The contract for issuing banks takes effect when signed, and is made for an indefinite period. It may be terminated by the issuing banks at any time. This is subject to fees stipulated in item 6. SignatureNet can terminate this contract with notice of three (3) months notice to the end of each calendar year.

11 Final provisions

The contract for issuing banks, together with any attachments, definitively governs the rights and duties between the contract partners. Oral agreements have no validity. Changes or supplements to this contract must be made in writing.

If a stipulation of these «GTCs for issuing banks» is shown to be null and void or legally ineffective, the other stipulations shall remain in force. In this case, the null-and-void or ineffective stipulation shall be replaced by an effective stipulation that corresponds as closely as possible in its economic effect to that of the ineffective stipulation.

09/2022 E