GENERAL TERMS AND CONDITIONS FOR ONLINE BANKING SERVICE

acme Online banking offers clients, on its Web site and with the agreement of the bank, an online service, hereafter referred to as the 'Service,' with allows for remote:

- Subscription to banking and non-banking services and products,
- Account consultation and management, in addition to the completion of banking operations

In the presently defined terms and conditions.

Service Usage

Access to the acme online service is completed through a terminal connected to an internet network.

acme is not responsible for any fees related to the acquisition or rental of the terminal, its installation and maintenance, or any network access and usage fees.

Service access and proof rules

The Service access and proof rules seek to specify and define the client's available means for completing online banking operations with acme's Internet. In this framework, and in order to allow for the use of online services, acme delivers Authenticators to clients, in the presently defined terms and conditions.

The Authenticators allow the Client to complete various operations, such as those described below in the terms and conditions stated in this present agreement:

- access the Service, in particular in order to view accounts,

- sign bank-related transactions,

- sign contractual or pre-contractual documents (agreements, forms…).

This agreement replaces the general conditions stated in the online banking contract, as well as the General Terms and Conditions of Individual Bank clients, the general conditions relating to each bank account agreement, and other concerned service or product contracts.

Definitions

The terms mentioned in this document that start with a capital letter or which are written in italics are defined as follows:

Client Identification: procedure that consists of recognizing the client in the acme information systems thanks to an Identifier.

Identifier: a piece of information sent to the client by acme, thereby allowing acme to be sure of a client's identity.

Client Authentication: procedure consisting of verifying, using appropriate methods, hereafter defined as Authenticators, the declared identity of the client. The authentication provides proof of the identity declared by the client during identification.

Authenticators: information or possessions belonging to the client, which can take the form of a personal access code, or private key associated with a certificate, allowing the acme information systems to complete the online authentication of the client. This list is not complete. The Authenticators can change over time, depending on the current technical standards, as long as the client is informed of any changes one (1) month in advance of the modifications.

Client Certificate: electronic document containing information that allows for the identification of the client, and attesting to the connection between the client and his or her private key. A certificate is electronically signed by acme, a recognized Certification Authority. acme therefore attests that the client whose identity is listed on the certificate is also in possession of his or her private key.

Client Private Key: a personal and confidential electronic document belonging to the client, which is conserved under the exclusive control of the client, and which is kept either on the client's computer or on a personal storage device. A private key is logically and irrevocably linked to the corresponding certificate.

Revocation: a procedure that consists of declaring that the client certificate and the private key are invalid, and therefore unusable. The client is therefore not responsible in the event of fraudulent use of the revoked certificate.

The Revocation of a certificate leads to the Revocation of all certificates issued by acme to the client.

Valid Client Certificate: characteristic of a certificate that is valid (not revoked), which is electronically signed by acme, as a Certification Authority.

Valid client certificates have a determined period of validity.

Certification Authority: The Certification Authority is an entity that provides certificate management services for the entire duration of a certificate, and which depends on a specific technical infrastructure, or Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI): all of the components and procedures used to manage the life cycle of electronic certificates.

The PKI uses these main functions to manage public key certificates:

- the recording of requests and verifications of attribution criteria,
- the creation and renewing of electronic certificates,
- the diffusion of certificates,
- the management of revocation lists,
- the archiving of certificates.

Delivery Procedure for Authenticators

The Authenticators delivered by acme are in the form of either a Personal Access Code or of a Valid Client Certificate.

Client Obligations

The client commits to respecting all of the security rules described below:

- respect and employ the security guidelines concerning the authentication methods, as outlined on the acme Security site. It is especially important that the code or the password is memorized (and not written down) and never shared with another individual, and that the certificate is stored on a personal computer.

- employ all methods available to ensure that the personal computer is reasonably secure

The responsibility of acme cannot be invoked in the event of hacking and / or fraudulent use of the client Authenticators caused by an error or negligence on the client's part, or in the event of a virus affecting the computer employed. The client therefore bears sole responsibility for any technical equipment that is used, as well as the use and conservation of the Authenticators, which should never be shared with anyone else.

Authenticators Use

Clients can use the Authenticators that have been given to them to:

- access acme services
- sign sensitive transactions
- sign pre-contractual or contractual documents, presented by acme in the framework of relations linking the client to the bank

Signing of sensitive transactions

After accessing an acme service, the client can complete a number of banking operations. In the event that the client tries to complete operations on his or her account, a summary of the operations requested is presented to the client, before the actions are carried out by acme, so that the client can confirm or cancel the actions.

Confirmation of the electronic signature operation

The summary of the operation is displayed in text format, through an electronic signature application which technically supports the electronic signature operation on the client computer. The client reads over the presented document. If the client then decides to confirm and validate the operation, he or she will choose the certificate to use for the transaction signature. The client must then check the box shown on the screen to confirm agreement, and click on the button 'Sign' before entering the security password for the certificate, which will activate the private key. The document is then electronically signed, and then sent to the acme information systems.

The acme information systems verify:

- that the signed document has not been modified since the signing, and that the client was in possession of the private key that corresponds to the certificate attached to the document,

- that the client certificate was valid at the time that acme received the document. This verification is done by validating the signature placed by acme on the presented certificate, by checking the dates of validity and by verifying that the certificate does not appear on any Certificate Revocation lists,

- that the document signed by the client is the same document that was presented to the client, without any modifications, other than the signature.

The operation requested by the client is authorized if all of these conditions are verified. If this is not the case, the operation will be refused. The document signed by the client, as well as the results of the verification and the information that was used the complete the verification are then returned in saved and timestamped files. These records are technically countersigned by the acme information system that completed the signature validation.

The client's electronic signature meets the conditions defined in the article 1316-4 of the Civil Code.

Signature of pre-contractual and contractual documents

After accessing the service (as described in article 4.1), in the framework of an acme service, the client may have the chance to sign up for other products and services offered by acme, giving rise to the signature of contractual documents. The client could also be required to access services needing the signature of pre-contractual documents such as questionnaires and other forms.

For the above mentioned cases, the acme information system will prepare a document to sign (depending on whether it is a sales proposal, a contractual document, or a form to sign), to which the acme electronic stamp will be affixed. The information system will then send the document to the client, who will then look over the document, complete it if necessary, and if appropriate, consent by signing the document.

The act of signing is presented as a PDF document, within the electronic signature application which technically supports the electronic signature operation on the client computer. The client looks over the presented document, and decides whether to sign or not. If the client decides to sign, he then chooses the certificate to use to sign the document, checks the box to confirm agreement, and clicks on the button 'sign.'

The document is then electronically signed in PDF format, and sent to the acme information systems.

The acme information systems verify:

- that the signed document has not been modified since the electronic signature was completed, and that the client was definitely in possession of the private key corresponding to the certificate attached to the document,

- that the client certificate was valid at the time that the signed document was received by acme. This verification is completed by validating the signature completed by acme on the certificate used, by checking the expiration date, and by verifying that the certificate does not appear on any certificate revocation lists,

- that the document signed by the client is the same document that was sent, without any modifications, additions, or deletions, other than the addition of the signature. This verification is completed by validating the electronic stamp that was completed by acme.

If these conditions are all verified, a PDF version of the document, with the electronic stamp of acme and the client electronic signature, is made available to the client. It can be stored on the client computer, or printed.

If these conditions are not verified, the document is destroyed and considered null and void.

The document signed by the client, as well as the results of the verification and the information that permitted this verification are then returned in the saved and timestamped files. These records are technically countersigned by the acme information system that completed the signature validation.

DURATION AND MODIFICATION

Duration and termination conditions

The acme service agreement is of an undetermined amount of time, and can be terminated be either party, at any time, with an advance notice of 15 days minimum, following written notice.

The closing of the account following the initiative of one of the parties will lead to the annulation of the agreement.

Modifications

The client can request that modifications be made to the agreement (specifically the list of accounts, and the amount of transfers). These will become effective with the acceptance of acme.

The service can be amended and the conditions of use are subject to change, especially in order to keep up with technological developments or improve the quality or security level of the services.

The client will be informed of these developments. The modifications will be considered as accepted by the client, except in the case of termination of the agreement in the appropriate time period.