Conditions applicables au transfert de données

Landesbank Saar
Ursulinenstraße 2, 66111 Saarbrücken

version 14 septembre 2019

1. Etendue de la prestation
(1) La banque offre à son client (titulaire de compte) n'ayant pas la qualité de consommateur la possibilité de procéder à des transferts de données par voie électronique – ci-après "transfert de données à distance" ou "TDD". Le transfert de données à distance comprend la transmission et la réception de données (en particulier la transmission d'ordres et l'obtention d'informations).
(2) La banque informe le client des types de services qui peuvent être rendus dans le cadre du transfert de données à distance. Les limites convenues avec la banque concernant le droit de disposer sont applicables à l'utilisation du transfert de données à distance.
(3) Le transfert de données à distance est possible selon la connexion EBICS (annexes 1a à 1c).
(4) La structure d'enregistrement et de fichier pour la transmission d'ordres et l'obtention d'informations est décrite à la rubrique « spécifications du format des données » (annexe 3).

2. Utilisateurs et participants, moyens d'authentification et de sécurisation
(1) Seul le client ou les personnes à qui il a donné pouvoir sur le compte peuvent passer des ordres au moyen de la connexion EBICS. Le client et ses mandataires sont ci-après ensembles désignés par "utilisateur". Chaque utilisateur a besoin de moyens d'authentification individuels activés par la banque pour que les données concernant un ordre transmis par TDD au moyen d'une signature électronique soient acceptées. Les exigences concernant les moyens d'authentification sont définies en annexe 1.a. Si cela est convenu avec la banque, l'authentification d'un ordre dont les données sont transmises par TDD peut résulter d'une note d'accompagnement/d'un ordre groupé signé(e).
(2) Pour l'échange de données par connexion EBICS, le client peut désig-
ner, outre des mandataires, des "participants techniques", qui sont unique- ment admis à réaliser l'échange de données. L'utilisateur et ses partici- pants techniques sont désignés ci-après par "participant". En vue de la sécurisation de l'échange de données, chaque participant a besoin de moyens de sécurisation individuels, activés par la banque. Les exigences concernant ces moyens de sécurisation sont décrites en annexe 1.a.

3. Procédure
(1) Selon la procédure de transfert convenue entre le client et la banque, sont applicables les exigences décrites à l'annexe 1a, ainsi que dans la documentation de l'interface technique (annexe 1b) et à la rubrique « spécifications du format des données » (annexe 3).
(2) Le client est tenu de s'assurer que tous les participants respectent les procédures et spécifications convenues avec la banque.
(3) Les champs de données doivent être remplis conformément aux directives applicables aux formats utilisés (annexe 3).
(4) L'utilisateur doit indiquer de façon exacte l'identifiant-client du bénéficiaire, ou le cas échéant du payeur, conformément aux conditions particulières respectivement applicables.
Les prestataires de service de paiement intervenant dans l'opération ne sont autorisés à traiter l'ordre que sur la base de l'identifiant-client. Les indications erronées peuvent conduire à une mauvaise exécution de l'ordre. Le client supporte seul les conséquences préjudiciables qui peuvent en résulter.
(5) Avant la transmission d'un ordre à la banque, il convient de procéder à l'enregistrement des fichiers à transmettre et de leur contenu complet, ainsi que des données transmises en vue du contrôle d'authentification. Sauf convention contraire, cet enregistrement doit être conservé par le client pendant une durée d'au moins 30 jours calendaires à compter de la date d'exécution indiquée dans le fichier (pour les virements), respectivement de la date d'échéance (prélèvements), ou en cas de pluralité de dates de la plus tardive d'entre elles, sous une forme telle que les fichiers puissent être mis à nouveau et à bref délai à la disposition de la banque, si elle le demande.
(6) En outre, pour chaque transmission et chaque réception de données, le client doit établir de façon automatisée un protocole, dont le contenu respecte les dispositions du chapitre 10 des spécifications pour la connexion EBICS (annexe 1b), de l'archiver et de le tenir à disposition de la banque sur sa demande.
(7) La banque n'est pas engagée par les informations qu'elle pourrait donner au client, concernant des opérations de paiement dont le traitement n'est pas achevé et définitif. De telles informations font l'objet d'une identification particulière.
(8) Les données relatives à un ordre transmises par TDD sont authentifiées, soit par une signature électronique, soit par une note d'accompagnement/un ordre groupé signé(e), selon ce qui a été convenu avec la banque. Ces données produisent les effets d'un ordre si,
a) en cas d'utilisation d'une signature électronique :
- toutes les signatures électroniques de l'utilisateur requises sont transmises par transfert de données à distance dans le délai convenu, et,
- les signatures électroniques ont pu être vérifiées avec succès au moyen des clés convenues,
ou
b) en cas de remise d'une note d'accompagnement/d'un ordre groupé :
- la note d'accompagnement/l'ordre groupé parvient à la banque dans le délai convenu, et
- la note d'accompagnement/l'ordre groupé est revêtu(e) de la signature de la personne ayant pouvoir sur le compte.

4. Obligations de diligence et de prudence concernant les moyens d'authentification en vue de l'admission de l'ordre
1) Le client est tenu de s'assurer que tous les participants respectent les obligations résultant des présentes conditions et la procédure d'authentification décrite en annexe 1a, selon le procédé de transfert convenu avec la banque.
(2) L'utilisateur peut donner des ordres, en recourant à l'un des moyens d'authentification activés par la banque. Le client doit s'assurer que chaque utilisateur prend toute mesure nécessaire afin qu'aucune autre personne n'entre en possession de ces moyens d'identification ou n'ait connaissance des mots de passe servant à leur protection. En effet, toute autre personne qui serait en possession du moyen d'identification ou d'un duplicata pourrait, avec le mot de passe correspondant, utiliser les services convenus d'une façon abusive.
Pour moyen d'authentification et du mot de passe, il convient notamment de veiller aux points suivants :
- le moyen d'authentification doit être protégé contre tout accès illégitime et conservé en sécurité ;
- le mot de passe servant à la protection du moyen d'authentification ne doit pas être noté sur le moyen d'authentification ou conservé en copie avec ce dernier ou encore stocké électroniquement sans mesure de sécurité ;
- le moyen d'authentification ne doit pas être dupliqué ;
- lors de la fourniture du mot de passe, il convient de s'assurer que d'autres personnes ne peuvent en prendre connaissance.

5. Obligations de diligence et de prudence liées au moyen de sécurisation pour l'échange de données
Dans le cadre de la connexion EBICS, le client doit s'assurer que tous les participants respectent la procédure de sécurité décrite en annexe 1a.
Le participant sécurise l'échange de données à l'aide des moyens de sécurisation activés par la banque. Le client doit donc s'assurer que chaque participant prend toutes les mesures nécessaires afin qu'aucune autre personne n'entre en possession de son moyen de sécurisation ou ne puisse l'utiliser. En particulier, en cas d'installation sur un système technique, le moyen de sécurisation du participant doit être stocké dans un environnement technique assurant la protection contre les accès non autorisés. En effet, toute autre personne qui aurait accès au moyen de sécurisation ou à un duplicata pourrait faire un usage abusif de l'échange de données.

6. Sécurité du système client
Il appartient au client de veiller à la sécurité des systèmes auxquels il recourt pour la transmission à distance. Les exigences en matière de sécurité applicables à la procédure EBICS sont décrites en annexe 1c.

7. Blocage des moyens d'authentification et de sécurisation
(1) Si les moyens d'authentification ou de sécurisation sont perdus, si une autre personne en a connaissance ou si leur utilisation abusive est soupçonnée, le participant doit immédiatement bloquer ou faire bloquer son accès TDD à la banque. Il convient de se référer à l'annexe 1a. Le partici-

manuell

pant peut transmettre son opposition à la banque à tout moment, notamment en utilisant les données de contact qui lui sont communiquées séparément.
(2) En dehors de la procédure de TDD, le client peut obtenir le blocage de l'utilisation des moyens d'authentification et de sécurisation d'un partici- pant, ou de la totalité de l'accès TDD, en observant la procédure d'opposition qui lui a été communiquée par la banque.
(3) La banque bloque totalement l'accès TDD lorsqu'existe un soupçon d'usage abusif de l'accès. La banque en informera le client en dehors de la procédure TDD. Ce blocage ne peut pas être levé par TDD.

8. Traitement par la banque des ordres entrant

(1) Les ordres transmis à la banque par le biais de la procédure TDD sont traités selon les procédures et délais habituels.
(2) La banque vérifie si l'émetteur est en droit de réaliser l'échange de données au moyen des signatures émises par les participants par le biais des moyens de sécurisation. Si cette vérification révèle des discordances, la banque ne traite pas les données d'ordre concernées et adresse immédiatement une information à ce sujet au client.
(3) La banque vérifie la légitimation de l'utilisateur, respectivement des uti-
lisateurs et l'authentification des données d'ordre transmises par TDD au moyen des signatures électroniques émises par les utilisateurs par le biais de leur moyen d'authentification ou de la note d'accompagnement/ de l'ordre groupé, ainsi que la concordance des données de l'ordre avec les stipulations de l'annexe 3. Si cette vérification révèle des discordances, la banque ne traite pas les données d'ordre concernées et adresse immédiatement au client une information. Après écoulement d'un délai communiqué séparément par la banque, celle-ci est en droit d'effacer les données relatives aux ordres non admis.
(4) Si lors des vérifications entreprises par la banque sont détectées des erreurs affectant les fichiers ou ensembles de données selon l'annexe 3, la banque conserve la preuve des fichiers ou ensembles de données défectueux dans une forme appropriée et en informe immédiatement l'utilisateur. La banque est en droit d'exclure les fichiers ou ensembles de données défectueux de tout traitement ultérieur, si l'exécution régulière de l'ordre ne peut pas être garantie.
(5) La banque doit consigner dans le protocole client les opérations (voir annexe 1a) et la transmission des ordres en vue de leur traitement. Le client doit prendre l'initiative de consulter le protocole client sans délai et s'informer du statut du traitement de l'ordre. En cas d'inexactitude, il doit se mettre en relation avec la banque.

9. Révocation

(1) Avant que les données d'un ordre ne soient acceptées, le client peut révoquer le fichier. La modification d'éléments particuliers d'un ordre suppose la révocation de l'entier fichier et une nouvelle transmission. La banque ne peut prendre en considération une révocation que si celle-ci lui parvient en temps utile, de telle sorte qu'il soit possible de lui donner effet dans le cadre du traitement normal des affaires.
(2) Le caractère révocable ou non d'un ordre est déterminé par les conditions particulières qui lui sont applicables (par exemple, les conditions applicables aux virements). La révocation des ordres peut intervenir en dehors de la procédure TDD ou selon les dispositions du chapitre 11 de l'annexe 3 si ceci est convenu avec le client. En vue de la révocation, le client doit communiquer à la banque toutes les indications relatives à l'ordre original.

10. Exécution des ordres

(1) La banque exécute les ordres quand toutes les conditions suivantes sont remplies :
- Les données d'ordre transmises par TDD ont été authentifiées conformément à l'article 3 alinéa 8.
- Le format des données est conforme.
- Les limitations du droit de disposer ne sont pas dépassées.
- Les conditions d'exécution propres à chaque type d'ordre, posées par les conditions particulières respectivement applicables, sont remplies (p. ex. une provision suffisante conformément aux conditions applicables aux virements).

(2) Si les conditions d'exécution fixées à l'alinéa 1 ne sont pas remplies, la banque n'exécute pas l'ordre et en informe immédiatement le client selon les modalités convenues. La banque indique autant que possible au client les raisons de la non-exécution et la façon d'y remédier.

11. Responsabilité

11.1 Responsabilité de la banque en cas d'ordre non autorisé, de non-exécution, d'exécution défectueuse ou tardive d'un ordre transmis par TDD
La responsabilité de la banque, qui exécute un ordre non autorisé, n'exécute pas ou exécute de façon défectueuse ou avec retard un ordre transmis par TDD est régie par les conditions particulières appli- cables aux types d'ordres considérés (p. ex. les conditions applicables aux virements).
11.2 Responsabilité du client en cas d'utilisation abusive ou fraudu- leuse des moyens d'authentification ou de sécurisation
11.2.1 Responsabilité du client en cas d'opérations de paiement non autorisées avant opposition
(1) Si avant l'opposition, des paiements ont lieu par suite d'une utilisation abusive ou frauduleuse d'un moyen d'authentification ou de sécurisation, le client est responsable des dommages occasionnés de ce fait à la banque si le participant a manqué, soit par négligence, soit intentionnellement à ses obligations de conduite et de prudence. Le § 675v du code civil allemand n'est pas applicable.
(2) Le client n'est pas tenu à réparation du dommage selon l'alinéa 1, si le dommage trouve sa cause dans l'impossibilité dans laquelle le participant s'est trouvé de faire opposition comme prévu à l'article 7 alinéa 1 du fait de la banque, qui n'a pas mis en œuvre les moyens de recevoir une telle opposition.
(3) Si le dommage a été causé alors qu'une limitation concernant le droit de disposer était en vigueur, le plafond fixé pour le droit de disposer s'applique également à la responsabilité.
(4) Les alinéas 2 et 3 ne sont pas applicables si le participant a agi avec une intention frauduleuse.
11.2.2 Responsabilité du client pour les autres opérations non autorisées réalisées avant opposition.
Si avant l'opposition, des opérations autres que des paiements ont lieu par suite d'une utilisation abusive ou frauduleuse d'un moyen d'authentification ou de sécurisation, quel qu'en soit le moyen, et notamment si celui-ci a été perdu ou volé, et qu'il en résulte un dommage pour la banque, le client et
la banque répondent des dommages conformément aux règles allemandes de la co-responsabilité.
11.2.3 Responsabilité de la banque après l'opposition.
Dès que la banque a réceptionné une opposition d'un participant, elle répond de tous les dommages provenant d'opérations non autorisées réa- lisées par TDD après l'opposition. Ceci ne s'applique pas toutefois si un participant a agi avec une intention frauduleuse.
11.3 Exclusion de responsabilité
La responsabilité est exclue si le dommage trouve sa cause dans des circonstances extraordinaires et imprévisibles, sur lesquelles la partie qui invoque ces circonstances n'avait aucune influence et dont elle n'aurait pas pu éviter les conséquences, même en faisant preuve de la vigilance et des soins requis.

12. Dispositions finales

Les annexes des présentes conditions font partie intégrante de l'accord conclu avec le client.
Annexe 1a : Connexion EBICS
Annexe 1b : Spécifications de la connexion EBICS
Annexe 1c : Exigences de sécurité concernant le système client - EBICS Annexe 2 : Actuellement inexistante
Annexe 3 : Spécifications du format de données

Annexe 1a : Connexion EBICS

1. Procédure d'authentification et de sécurisation

Le client (titulaire du compte) désigne à la banque les participants et leurs ayants droit pour la transmission de données à distance. Les procédures suivantes d'authentification et de sécurisation sont instaurées dans le cadre de la connexion EBICS :

- Signature électronique
- Signature d'authentification
- Verrouillage

Pour chaque procédure d'authentification et de sécurisation, le participant dispose d'une paire de clés individuelles constituée par une clé privée et une clé publique. Les clés publiques des participants doivent être communiquées à la banque conformément à la procédure décrite à l'article 2. Les clés publiques de la banque doivent être protégées contre toute modification non autorisée, conformément à la procédure décrite à l'article 2. Les paires de clés du participant peuvent être utilisées pour les besoins de la communication avec d'autres banques.

1.1 Signatures électroniques des participants

Pour les signatures électroniques (SE) des participants, les classes de sig- nature suivantes sont définies :

- Signature unique (Type "E")
- Première signature (Type "A")
- Deuxième signature (Type "B")
- Signature de transport (Type "T")

Les signatures électroniques bancaires sont celles de type E, A ou B. Les signatures électroniques bancaires permettent la passation d'ordres. Les ordres peuvent nécessiter plusieurs SE bancaires qui doi- vent émaner de différents utilisateurs (titulaires de compte leurs mandataires). Pour chaque type d'ordre, il est convenu entre la banque et le client d'un nombre minimum de SE bancaires obligatoires. Les SE de type T, qui sont des signatures de transport, ne sont pas utilisées pour la passation d'ordres bancaires, mais seulement pour leur trans- mission au système bancaire. Les "participants techniques" (voir art. 2.2.) ne peuvent obtenir qu'une SE de type T. Le logiciel utilisé par le client permet l'émission de différents messages (par exemple des ordres de paiement domestiques ou vers l'étranger, mais aussi ceux liés à l'initialisation, à l'accès au protocole et aux informations concernant le compte et les opérations réalisées, etc.). La banque communique au client les types de message qui peuvent être utilisés et les types de signature électronique correspondants.

1.2 Signature d'authentification

Au contraire de la SE, qui vaut signature des ordres, la signature d'authentification est formée par chaque message EBICS incluant les don- nées d'orientation et d'authentification ainsi que la SE qui y est comprise. La signature d'authentification est utilisée pour chaque étape de la transaction, tant par le client que par le système bancaire, à l'exception de certains types d'ordres ou de transmissions inhérents au système, définis dans les spécifications EBICS. Le client doit garantir qu'il a installé un logiciel assurant la vérification de la signature d'authentification de chaque message EBICS transmis par la banque, cette vérification portant également sur le caractère actuel et authentique de la clé publique stockée par la banque conformément aux clauses des spécifications EBICS (voir annexe 1b).

1.3 Encodage

Pour préserver le secret des données bancaires lors de leur utilisation, les données d'ordres doivent être encodées par le client conformément aux spécifications EBICS (voir annexe 1b) et en s'assurant du caractère actuel et authentique de la clé publique de la banque.

En outre, il convient de procéder à un encodage de transport pour les transferts externes entre le client et le système bancaire. Le client doit garantir que le logiciel qu'il a installé vérifie le caractère authentique du certificat de serveur mis en place à cette fin par la banque, conformément aux spécifications EBICS (voir annexe 1b).

2. Initialisation de la connexion EBICS

2.1 Mise en place de la liaison de communication

La communication est établie au moyen d'une URL (Uniform Resource Locator). Il est également possible d'utiliser une adresse IP de la banque respective. L'URL ou l'adresse IP sont communiqués au client à la conclusion du contrat avec la banque.

Pour la mise en place de la connexion EBICS, la banque communique aux participants désignés par le client les données suivantes :

- URL ou adresse IP de la banque aux fins d'établissement de la communication
- désignation de la banque
- HostID
- version(s) admise(s) pour le protocole EBICS et la procédure de sécurité
- ID du partenaire (ID - client)
- User-ID
- system-ID (pour les participants techniques)
- d'autres indications spécifiques liées à la légitimation du client et des participants

La banque attribue à chaque participant affilié au client un identifiant d'utilisateur (user–ID) qui permet d'identifier avec certitude ce participant. Lorsqu'un ou plusieurs participants techniques sont affiliés au client (multi- user-system), la banque attribue, outre le user-ID, un identifiant système (system-ID). Si aucun participant technique n'est désigné, system-ID et user-ID sont identiques.

2.2. Initialisation des clés de participants

Les paires de clés installées par le participant en vue de la SE bancaire, l'encodage des ordre et les signatures d'authentification doivent satisfaire aux exigences suivantes, outre les conditions générales décrites à l'article 1 :

1. Les clés de signature sont attribuées de façon exclusive et indubitable au participant
2. Si le participant génère lui-même ses clés, les clés privées doivent être créées avec des moyens détenus par le participant sous son contrôle exclusif.
3. Si les clés sont mises à disposition par un tiers, il convient de s'assurer que le participant a la possession exclusive de la clé privée.
4. Pour chaque clé privée installée aux fins de légitimation, chaque participant définit un mot de passe qui sécurise l'accès à la clé privée concernée.
5. Pour chaque clé privée installée aux fins de sécurisation de l'échange de données, chaque participant définit un mot de passe qui sécurise l'accès à la clé privée concernée. Il est possible de renoncer à ce mot de passe si le moyen de sécurisation du participant est stocké dans un environnement technique assurant la protection contre les accès non autorisés.

Pour initialiser le participant auprès de la banque, il est indispensable de transmettre la clé publique du participant à la banque. Pour cela, le participant transmet à la banque sa clé publique par deux moyens de communication distincts l'un de l'autre :

- par la connexion EBICS au moyen des types d'ordre prévus par le système à cet effet,
- au moyen d'une lettre d'initialisation signée par le titulaire du compte ou par son mandataire.

Pour valider l'accès du participant, la banque vérifie l'authenticité de la clé publique du participant transmise par EBICS sur la base de la lettre d'initialisation signée par le client ou par son mandataire.

Pour chaque clé publique de participant, la lettre d'initialisation comporte les données suivantes :

- Utilisation assignée à la clé publique de participant
  - Signature électronique
  - Signature d'authentification
  - Encodage
- version retenue pour chaque paire de clés
- indication de longueur de l'exposant
- exposant de la clé publique en notation hexadécimale
- indication de longueur du modulus
- modulus de la clé publique en notation hexadécimale
- valeur hachée de la clé publique en notation hexadécimale.

La banque vérifie la signature du titulaire du compte et le cas échéant de son mandataire qui figure sur la lettre d'initialisation ainsi que la concordance entre les valeurs hachées transmises par connexion EBICS et par écrit de la clé publique du participant. Si le résultat de cette vérification est positif, la banque valide l'accès du participant concerné pour les types d'ordre convenus.

2.3 Initialisation de la clé de la banque

Le participant se fait délivrer la clé publique de la banque en exécutant l'un des types d'ordre prévus par le système à cet effet. La valeur hachée de la clé publique de la banque est en outre communiquée par un autre mode de communication convenu séparément avec le client.

Avant la première utilisation EBICS, le participant doit vérifier l'authenticité de la clé publique de la banque qui lui a été transmise par voie de transfert de données à distance en comparant sa valeur hachée avec la valeur hachée qui lui a été communiquée par le mode de communication con- venu séparément.

Le client doit garantir qu'il a procédé à l'installation d'un logiciel assurant la vérification de la validité du certificat de serveur installé dans le cadre du chiffrement de transport au moyen du chemin de certification commu-

niqué séparément par la banque.

3. Obligations particulières de prudence en cas de production de moyens d'authentification et de sécurisation par le client

Lorsque le client produit lui-même ses moyens d'authentification et de sécurisation selon les spécifications EBICS et qu'il les initialise auprès de sa banque, il doit veiller à ce qui suit :

- La confidentialité et l'intégrité du moyen d'authentification dans toutes les phases de l'authentification, y compris la notification, la transmission et le stockage, doivent être garanties.
- Les clés de participants privées des moyens d'authentification et de sécurisation ne doivent pas être stockées en texte clair.
- Le moyen d'authentification est bloqué au plus tard après cinq indications erronées successives du mot de passe.
- La génération des clés de participants publiques et privées doit avoir lieu dans un environnement sûr.
- Les moyens d'authentification et de sécurisation doivent être rattachés exclusivement et sans équivoque au participant et utilisés par lui seul.

4. Transmission d'ordres à la banque

L'utilisateur vérifie l'exactitude des données de l'ordre et s'assure que ces mêmes données soient signées électroniquement. Lors de l'établissement de la communication, la banque vérifie tout d'abord les éléments de légiti- mation concernant le participant, comme par exemple le droit de donner ce type d'ordre ou le cas échéant le respect des limites convenues. Le résultat des vérifications incombant à la banque, comme par exemple les vérifications concernant les limites de pouvoir, ou la capacité relativement au compte, est communiqué ultérieurement au client par le biais du protocole client.

Les ordres transmis au système de la banque peuvent être autorisés selon les modalités suivantes :

1. Toutes les signatures électroniques bancaires requises sont transmises en même temps que les données d'ordre.
2. S'il a été convenu avec le client pour le type d'ordre concerné d'une signature électronique partagée (SEP) et que les signatures électroniques transmises ne sont pas suffisantes, l'ordre est stocké et mis en attente jusqu'à la transmission de toutes les SE nécessaires.
3. S'il est convenu entre le client et la banque que l'authentification des données d'ordres transmises par TDD est effectuée par le biais d'une note d'accompagnement/d'un ordre groupé transmis(e) séparément, c'est une signature de transport (de type "T") qui est requise à la place de la signature électronique bancaire de l'utilisateur. Le fichier doit alors être signalé par une identification spéciale qui indique qu'en dehors de la signature de transport (de type "T") il n'y a pas d'autre signature électronique pour cet ordre. Il est donné suite à l'ordre si la vérification par la banque de la signature de l'utilisateur figurant sur la note d'accompagnement/ l'ordre groupé est positive.

4.1 Passation d'ordres par le biais d'une signature électronique partagée (SEP)

Les modalités d'utilisation par le client d'une Signature Electronique Partagée doivent être convenues séparément avec la banque. Il est recouru à la Signature Electronique Partagée (SEP) si l'autorisation des ordres doit intervenir indépendamment du transfert des données relatives aux ordres et le cas échéant si elle doit être donnée par plusieurs participants. Tant que toutes les signatures électroniques bancaires requises pour l'autorisation ne sont pas données, l'ordre peut être annulé par l'un des utilisateurs autorisés. Lorsque l'ordre a été autorisé de façon complète, une révocation n'est possible que dans les conditions prévues à l'article 9 des Conditions applicables au transfert de données.
La banque est en droit d'annuler un ordre qui n'a pas été autorisé de façon
complète à l'expiration du délai qu'elle a communiqué de façon séparée.

4.2 Vérification de légitimation par la banque

Les données d'ordres transmises par TDD ne sont exécutées en tant qu'ordres par la banque que lorsque celle-ci a réceptionné les signatures électroniques bancaires requises, respectivement le billet d'accompagnement/l'ordre groupé signé, et que ces derniers ont été vérifiés avec succès.

4.3 Protocole client

La banque consigne dans un protocole client les processus suivants :
- Transmission des données d'ordres au système automatisé de la banque
- Transmission de fichiers d'information par le système de la banque au système du client
- Résultat du contrôle de légitimation portant sur les ordres transmis par le client au système de la banque
- Traitement ultérieur des ordres pour autant que ces derniers concernent la vérification de signatures et la notification des données d'ordre.

Le participant doit s'enquérir du résultat des vérifications entreprises par la banque dans les meilleurs délais, en consultant le protocole client.
Le participant doit archiver ce protocole, dont le contenu correspond aux stipulations du chapitre 10 de l'annexe 1b et doit le tenir à la disposition de la banque sur demande de sa part**.**

5. Modification de la clé d'un participant avec validation automatique

Si la validité des moyens de légitimation et de sécurisation mis en place par un participant est limitée dans le temps, le participant doit transmettre à sa banque les nouvelles clés publiques de participant suffisamment à l'avance, avant la date d'expiration. Après dépassement de la date de validité des vieilles clés, une nouvelle initialisation doit être effectuée.
Si le participant génère lui-même ses clés, il doit renouveler les clés de participant au moment convenu avec la banque en exécutant l'un des types d'ordre prévus par le système à cet effet et les transmettre suffisamment à temps avant que les vieilles clés ne soient périmées.
Pour obtenir une validation automatique des nouvelles clés sans procéder à une nouvelle initialisation, les procédures suivantes doivent être observées :
- actualisation de la clé publique bancaire (PUB) et
- actualisation de la clé publique d'authentification et de la clé publique de chiffrage (HCA)

ou, alternativement
- actualisation de chacune des trois clés citées ci-dessus (HCS).

Les procédures PUB et HCA, respectivement HCS supposent l'utilisation d'une SE bancaire valable de l'utilisateur. Après accomplissement de la modification, seules les nouvelles clés doivent être utilisées.
Si la signature électronique n'a pas pu être vérifiée avec succès, il sera procédé comme indiqué à l'article 8 alinéa 3 des Conditions applicables au transfert de données.
Le changement de clés ne peut intervenir qu'après traitement complet de tous les ordres. A défaut, les ordres non complètement exécutés doivent être renouvelés avec la nouvelle clé.

6. Blocage de la clé de participant

S'il est soupçonné qu'une clé de participant a été abusivement utilisée, le participant est tenu de faire bloquer ses droits d'accès à tous les systèmes de la banque qui utilisent la ou les clés compromises. Si le participant dispose de moyens de légitimation et de sécurisation valables, il peut procéder à ce blocage par connexion EBICS. L'envoi d'un message de type "SPR" emportera le blocage de l'accès du participant (identifié par son "User-ID") auteur de l'envoi du message. Après un blocage et jusqu'à la nouvelle initialisation décrite à l'article 2, aucun ordre ne peut plus être donné par ce participant par le biais de la connexion EBICS.
Si le participant ne dispose plus de moyens de légitimation et de sécurisation valables, il peut faire bloquer ses moyens de légitimation et de sécurisation en dehors de la procédure TDD, par les moyens communiqués séparément par la banque.
Le client peut faire bloquer en dehors de la procédure TDD et par les procédés d'opposition communiqués séparément par la banque les moyens de légitimation et de sécurisation d'un participant ou la totalité de l'accès TDD.

Annexe 1b :

Spécifications de la connexion EBICS.
Les spécifications sont publiées sur le site Internet www.ebics.de.

Annexe 1c :

Conditions tenant à la sécurité du système EBICS du client
Outre les mesures de sécurité décrites à l'annexe 1a article 5, les exigences suivantes doivent être respectées par le client :
- Le logiciel installé par le client pour la procédure EBICS doit respecter les exigences décrites à l'annexe 1a.
- Les systèmes EBICS du client ne doivent pas être installés sans un pare-feu (firewall). Un pare-feu est un système qui surveille la circulation des messages entrant et sortant et n'autorise que les contacts connus ou autorisés.

- Un scanner de virus doit être installé, qui est régulièrement alimenté avec les fichiers de définition de virus les plus récents.
- Le système EBICS du client doit être installé de telle façon que le participant soit tenu de se signaler avant son utilisation. Cette signalisation doit être faite en tant qu'utilisateur normal, et non pas en tant qu'administrateur, qui serait par exemple en droit de décider de l'installation de programmes.
- Les moyens de communication électronique internes utilisés pour des données bancaires non chiffrées ou pour des messages EBICS non

chiffrés doivent être protégés contre toute captation et manipulation.
- S'il existe des mises à jour ou nouvelles versions concernant la sécurité du système installé, et d'autres logiciels installés concernant la sécurité, le système EBICS du client doit être actualisé par ce biais.
Il est de la responsabilité exclusive du client de transposer ces exigences.

Annexe 2 :
Sans objet à ce jour.

Annexe 3 :
Spécification du format des données
La spécification est publiée sur le site Internet www. ebics.de.