

Abacus  
Guide d'installation

**Electronic Banking**  
**EBICS**

Dès la version 2015

**février 18 / uth / fha**

Cette documentation est protégée par des droits d'auteur.

En particulier, le droit de copier, exposer, distribuer, traiter, traduire, transmettre ou enregistrer une partie ou l'ensemble du support par n'importe quel média (sous forme graphique, technique, électronique et/ou digitale, y inclus la photocopie et le téléchargement en ligne) est strictement réservé à Abacus Research SA.

Toute utilisation dans les cas mentionnés ou dans les cas autres que ceux autorisés par la loi, notamment toute utilisation commerciale, requiert auparavant un accord par écrit d'Abacus Research SA.

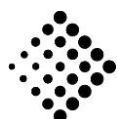
D'après l'art. 67 al. 2 LDA, la violation par métier des droits d'auteurs peut être sanctionnée.

Copyright © 2018 by Abacus Research SA, CH-9301 Wittenbach-St Gall

# Sommaire

---

<b>1</b>	<b>Avant l'installation .....</b>	<b>2</b>
1.1	Protocole soutenu .....	3
1.2	Restrictions d'Abacus .....	3
1.3	Mise à jour EGI.....	4
1.4	Importation EGI .....	4
<b>2</b>	<b>Paramètres de communication .....</b>	<b>5</b>
<b>3</b>	<b>Installer EBICS.....</b>	<b>7</b>
3.1	Choix du serveur de communication et du proxy .....	7
3.2	Sélection établissement .....	8
3.3	Attribution du contrat .....	9
3.4	Définition du contrat .....	10
3.5	Initialisation.....	11
3.6	Validation des clés bancaires par l'établissement financier .....	12
3.7	Chercher/télécharger les clés bancaires.....	13
3.8	Confirmation clé bancaire / accepter Hash .....	15
3.9	Activer Recevoir types d'ordre et Envoyer types d'ordre .....	16
<b>4</b>	<b>Annexe – Exemple de lettre INI .....</b>	<b>17</b>
<b>5</b>	<b>Annexe – Exemple de lettre HIA .....</b>	<b>18</b>



## 1 Avant l'installation

### Documents importants et interlocuteurs

- ✓ Assurez-vous que les contrats correspondants existent. Vous ne recevez par EBICS aucunes clés physiques mais différents documents avec les données correspondantes.
- ✓ L'administrateur Abacus et le responsable du réseau devraient être joignables.

### Sécurité

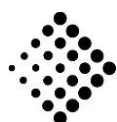
Abacus Electronic Banking vous offre une variété de mécanismes de sécurité tels que le cryptage SSL de toutes les communications, le cryptage de toutes les données envoyées et reçues, les différentes méthodes d'authentification, les requêtes de mot de passe, le contrôle des signatures, etc.

### Attention

L'accès au répertoire abac, aux données du contrat et aux clés bancaires devrait être limité. Les personnes non autorisées ne devraient avoir aucun libre accès à votre système. Chaque client est responsable de l'accès interne aux documents du contrat, aux disquettes-clés et aux mots de passe.

Malgré les mécanismes de sécurité énumérés ci-dessus, il est essentiel d'examiner les mesures de sécurité informatique et de protéger l'environnement informatique, le réseau et le matériel contre les attaques externes. Il est vrai que des attaques contre la communication entre l'Electronic Banking et les établissements financiers peuvent être exclues. Cependant, si l'environnement informatique ou une partie de celui-ci est infecté par un logiciel malveillant, certains processus pourraient néanmoins être surveillés et, dans des cas extrêmes, manipulés. De plus amples informations sont à disposition sur le site Web de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI :

<https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/offline-payment-software.html>



# Avant l'installation

---

## 1.1 Protocole soutenu

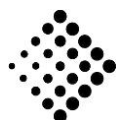
EBICS est soumis à de sévères règles concernant la version à mettre en place. De plus, il existe différents procédés pouvant être appliqués. Les informations suivantes vous montrent ce qui en ce moment est soutenu par Abacus :

Protocole : H004  
Signature : A005  
Authentification : X002  
Encryption : E002

Version actuelle EBICS d'Abacus : V2.5

## 1.2 Restrictions d'Abacus

- La signature électronique distribuée (VEU) n'est PAS soutenue. Un contrat avec signature individuelle doit être commandé auprès de l'établissement financier.
- Il ne doit y avoir qu'un seul utilisateur (corporate sealing). Il n'y a donc aucun besoin d'un utilisateur de transport.
- Les banques EBICS peuvent définir en option (pas standard) des classes de signatures sélectives par type de session ainsi que leurs limites. Cependant, Abacus ne soutient pas ceci.
- Les certificats Hardware (avec ou sans PinPad) ne sont pas soutenus.




## 1.3 Mise à jour EGI

L'Electronic Banking soutient différentes interfaces. Les établissements financiers sont affectés à l'interface correspondante via la mise à jour EGI. Il est recommandé de toujours exécuter la mise à jour EGI avant de créer un nouvel établissement.

La dernière mise à jour EGI peut être téléchargée de la page suivante :

<http://classic.abacus.ch/fr/downloads-page/autres-documents-dapplications/electronic-banking/>



Electronic Banking

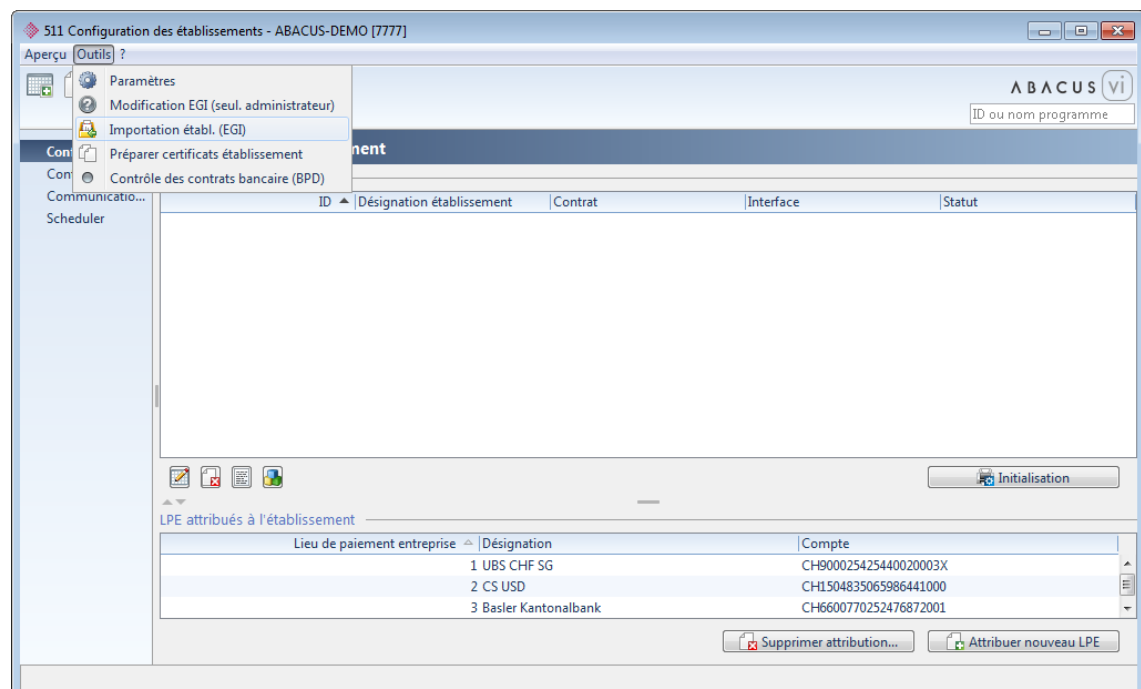
Autres documents d'applications > Electronic Banking

Nom du fichier	Taille	Date de création
Installation instituts financiers V2011 / 2012 (PDF)	5 MB	21.02.2014
Liste des établissements bancaires (HTML)	56 Kbyte	22.02.2017
Guide d'installation EBICS (PDF)	1.1 MB	16.02.2016
Update EGI (ZIP)	9 Kbyte	22.02.2017

Harmonisation du trafic des paiements en Suisse ISO 20022

L'Electronic Banking, tout comme l'ensemble des logiciels ABACUS, est indépendant de la plate-forme. Cela signifie que tous les établissements financiers, figurant dans la liste des banques avec une interface, peuvent être configurés sous Windows, Apple et Linux. À l'exception des interfaces Intersystem (CLX) et UBS Key Direct. Ces deux interfaces se basent sur des composants Windows. Le serveur de communication ABACUS doit donc être installé sur un ordinateur Windows pour ces interfaces.

## 1.4 Importation EGI



S11 Configuration des établissements - ABACUS-DEMO [7777]

Outils ?

- Paramètres
- Modification EGI (seul administrateur)
- Importation établ. (EGI)
- Préparer certificats établissement
- Contrôle des contrats bancaire (BPD)

ID	Désignation établissement	Contrat	Interface	Statut

Initialisation

LPE attribués à l'établissement

Lieu de paiement entreprise	Désignation	Compte
1	UBS CHF SG	CH900025425440020003X
2	CS USD	CH1504835065986441000
3	Basler Kantonalbank	CH6600770252476872001

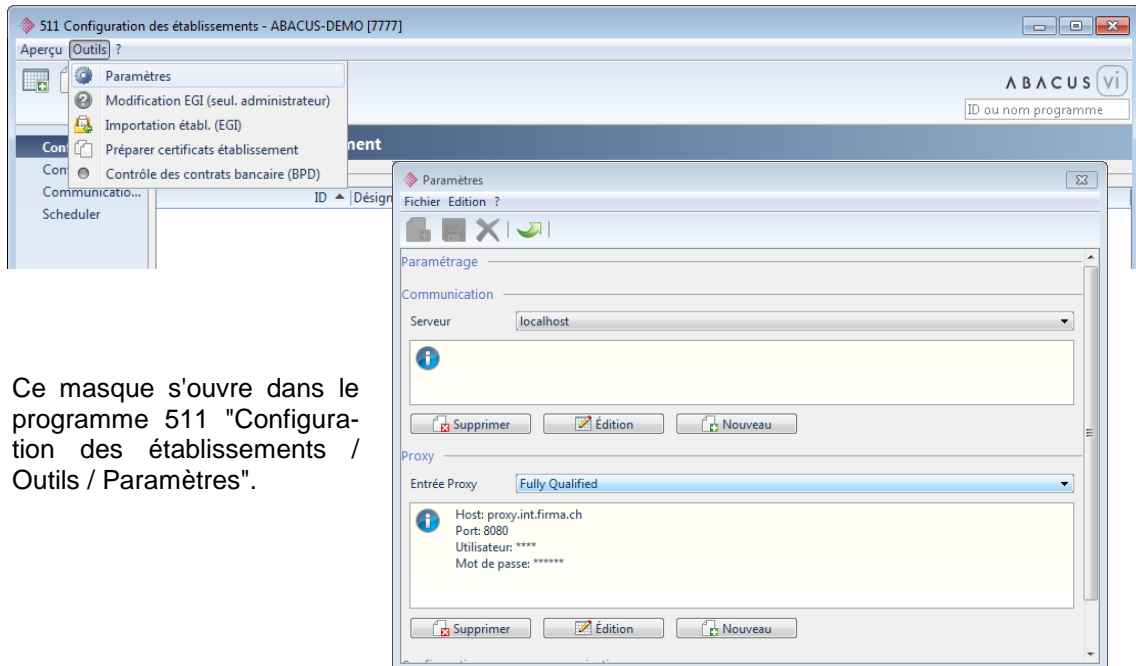
Supprimer attribution... Attribuer nouveau LPE

Pour effectuer la mise à jour EGI, le fichier XML téléchargé doit être extrait de l'archive ZIP et importé dans le programme 511 "Configuration des établissements / Outil / Importation établ. (EGI)".



## 2 Paramètres de communication

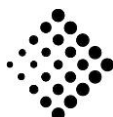
Les paramètres de communication doivent être enregistrés ou éventuellement retravaillés avant la configuration des établissements.



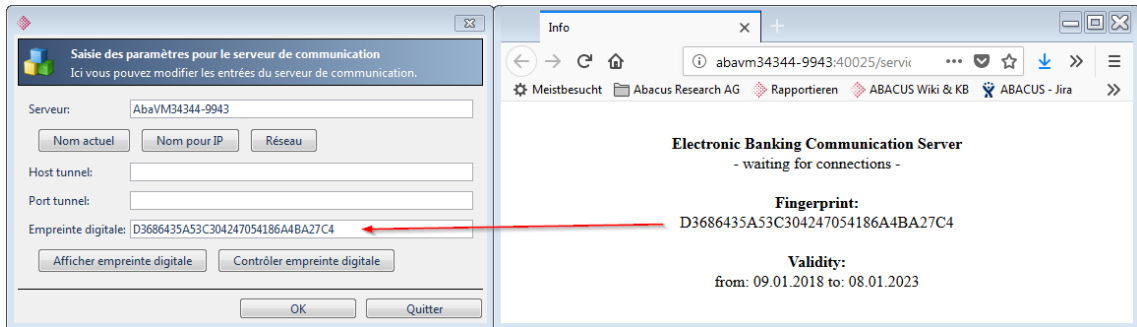
Ce masque s'ouvre dans le programme 511 "Configuration des établissements / Outils / Paramètres".

Sous "Serveur", vous pouvez ajouter un nouveau serveur de communication à l'aide du bouton <Nouveau> ou en modifier un existant à l'aide du bouton <Édition>. Si un serveur existant n'est plus utilisé, vous pouvez le sélectionner puis le retirer avec <Supprimer>.

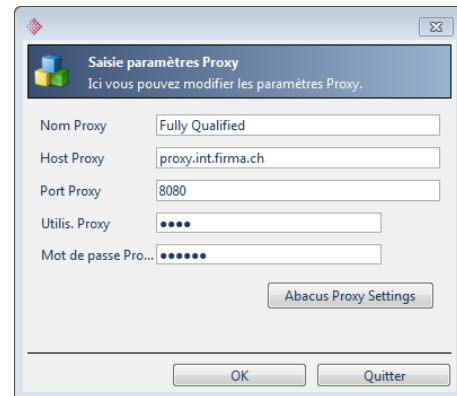
Normalement, le serveur de communication correspond à l'ordinateur sur lequel Abacus est installé. Dans ce cas, cliquez sur le bouton <Nom actuel>. Si le serveur n'est pas trouvé grâce au nom (DNS), le bouton <Nom pour IP> permet de déterminer son adresse IP. Si la communication se fait au moyen d'un serveur de communication externe, vous pouvez le rechercher à l'aide du bouton <Réseau> ou saisir manuellement le nom resp. l'adresse IP.



Une empreinte digitale (fingerprint) doit obligatoirement être enregistrée pour chaque entrée de serveur. Elle est appelée avec le bouton <Afficher fingerprint>. Une fenêtre de navigateur (p. ex. Internet Explorer ou Firefox) s'ouvre alors et l'empreinte digitale peut être copiée puis collée dans le champ correspondant. En cliquant ensuite sur le bouton <Contrôler Fingerprint> vous vérifiez que l'empreinte digitale est correcte.

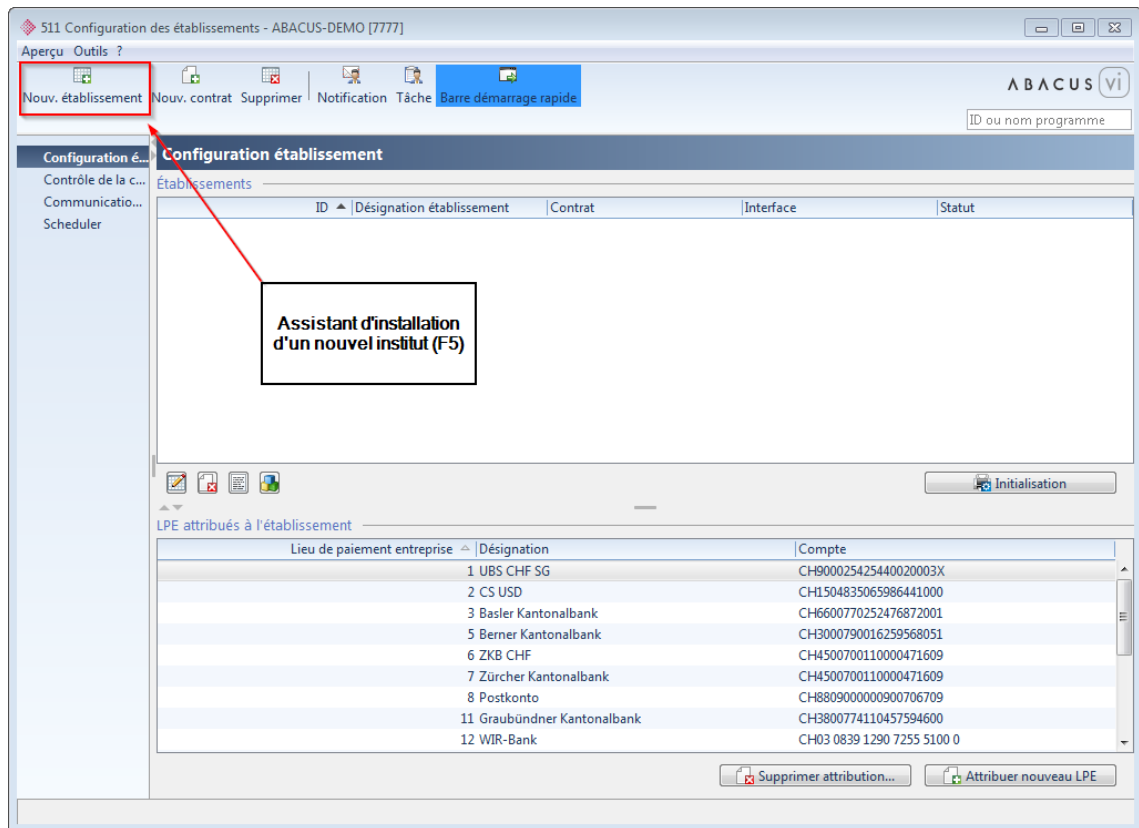


Si un proxy est utilisé pour la liaison Internet et qu'il est éventuellement protégé par un nom d'utilisateur et un mot de passe, vous pouvez ajouter une nouvelle entrée proxy grâce au bouton <Nouveau> ou en modifier une existante grâce à <Édition> dans la partie Proxy. Si une entrée proxy existante n'est plus utilisée, vous pouvez la sélectionner puis la retirer avec <Supprimer>.



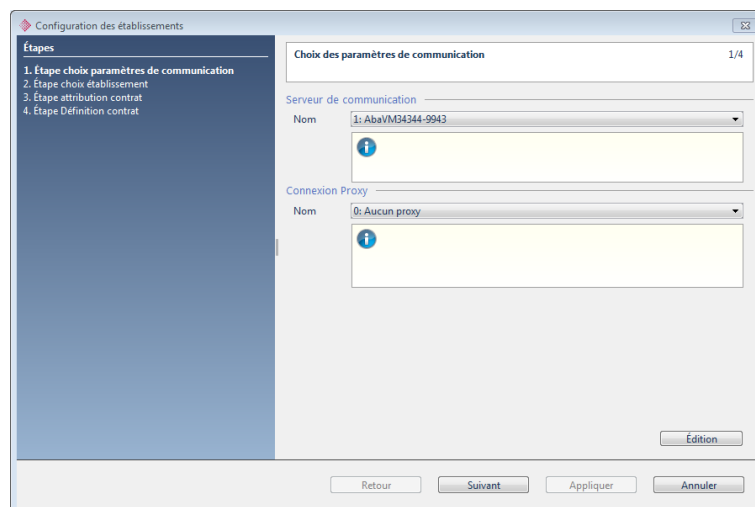
### 3 Installer EBICS

L'installation d'un nouvel établissement commence toujours par l'ouverture de l'assistant via le bouton correspondant.



#### 3.1 Choix du serveur de communication et du proxy

Vous devez sélectionner ici le serveur de communication et l'éventuelle entrée proxy. Si nécessaire, vous pouvez indiquer ou modifier ces paramètres à l'aide du bouton <Édition> (voir Paramètres de communication dès en page 5.)





## 3.2 Sélection établissement

 **Attention**

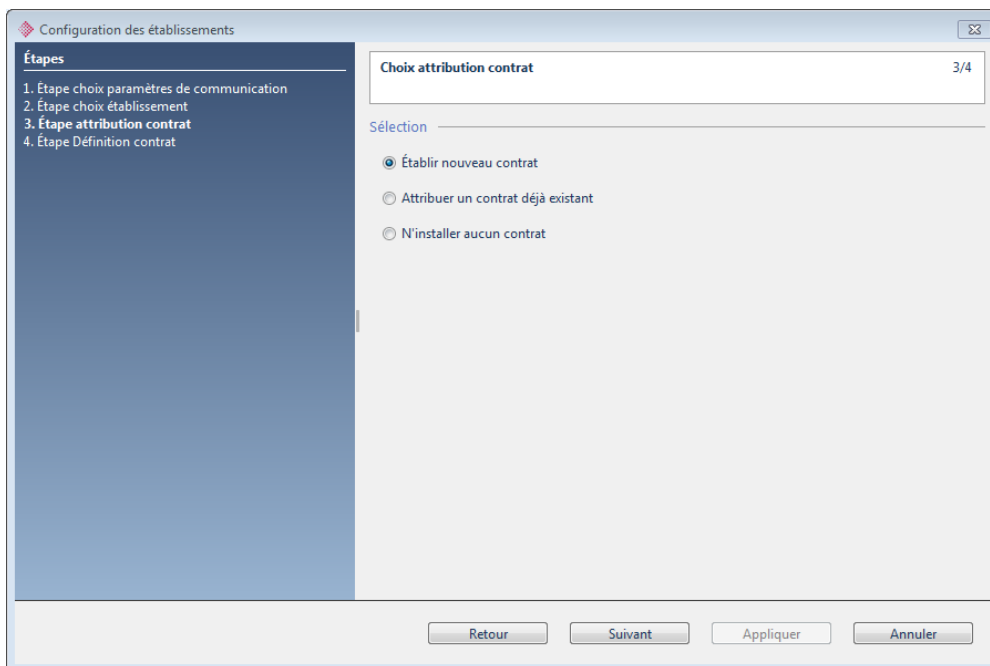
Les établissements avec une interface EBICS doivent toujours être installés avec l'établissement financier 2 "EBICS". Si un établissement (par ex. UBS) est affiché dans la liste des établissements bancaires avec une interface EBICS, ce n'est qu'à titre informatif.

 **Descriptions des champs**

- Établissement financier** Choisir l'établissement financier 2 "EBICS". À l'encontre d'autres interfaces, ce n'est pas l'établissement qui est directement sélectionné mais l'interface.
- Pays** Sélectionnez ici le pays où se trouve l'établissement.
- Version Sepa** Les versions Sepa sont différentes de pays en pays. Il faut choisir ici la version supportée par l'établissement.
- Désignation** Le choix de la désignation est libre. Il est important, avec plusieurs établissements, de choisir des désignations explicites (par ex. le nom de l'établissement financier) afin de les discerner ultérieurement les uns des autres.
- Interface** L'interface EBICS est automatiquement renseignée. Sinon, il faut effectuer une Mise à jour EGI (voir en page 4).
- Statut** Le statut "Installer" doit rester. Il passe automatiquement à "En service" une fois l'installation terminée.
- Avis de débit global SEPA** Cette case est activée si une écriture collective doit être créée par niveau B (Payment Information) dans pain.001. (Batch Booking = true). Il faut vous informer auprès de l'établissement financier, si Batch Booking est soutenu. SIX conseille par contre de cocher cette case.



## 3.3 Attribution du contrat

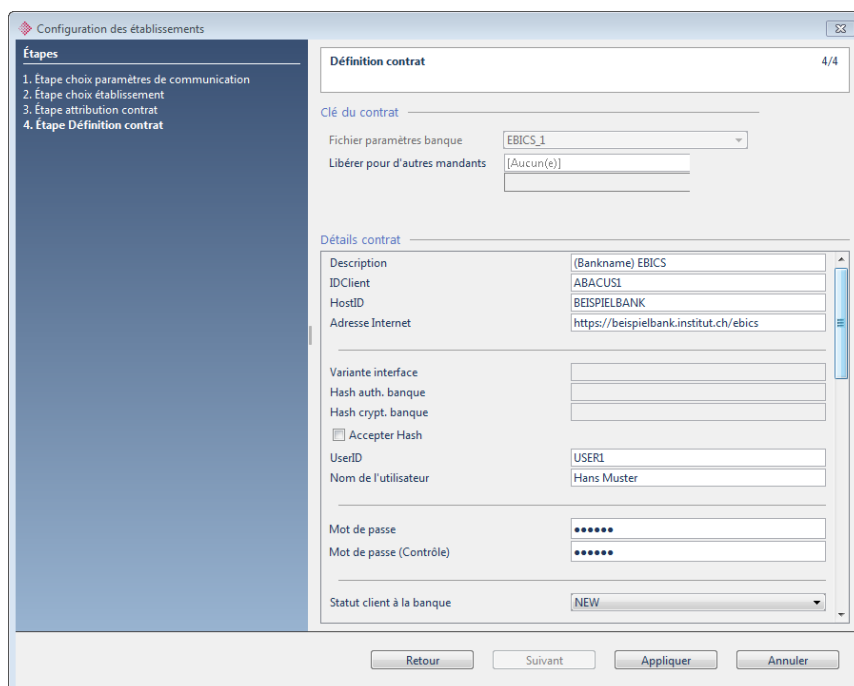


### Descriptions des champs

- |                                    |  |
|------------------------------------|--|
| Établir nouveau contrat            | Créez un nouveau contrat s'il n'existe ni établissement ni contrat pour cette banque dans ce mandant.  |
| Attribuer un contrat déjà existant | Sélectionnez cette option si le contrat a déjà été importé (contrats communs aux mandants) et si vous désirez ouvrir un établissement financier pour ce contrat. |
| N'installer aucun contrat          | Un établissement est créé sans contrat. Une communication en ligne n'est pas possible par la suite.  |



### 3.4 Définition du contrat



#### Descriptions des champs

##### Libérer pour d'autres mandants

Vous pouvez définir ici si ce contrat doit aussi être libéré pour d'autres mandants.

##### IDClient

ID client selon les documents du contrat. Elle peut être identique à l'ID utilisateur.

##### Adresse Internet

URL de l'établissement selon les documents du contrat.

##### Nom d'utilisateur

Prénom et nom de la personne figurant dans le contrat EBICS.

##### Statut client à la banque

Pour l'initialisation, le statut du client doit être "NEW".

##### Description

Désignation explicite et librement définissable pour le contrat.

##### HostID

Host ID de l'établissement selon les documents du contrat.

##### UserID

ID utilisateur selon les documents du contrat. Elle peut être identique à l'ID client.

##### Mot de passe

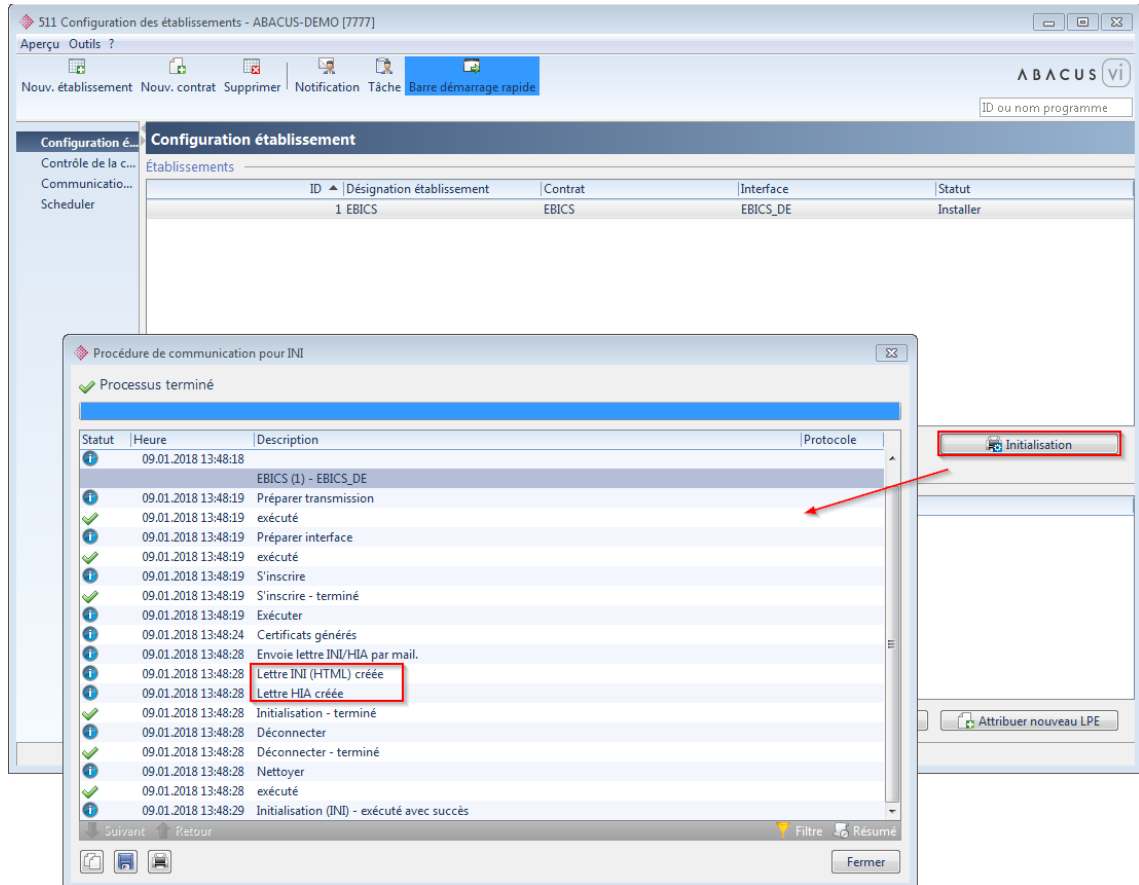
Introduisez le mot de passe librement définissable (min. 6 caractères) et répétez-le sous "Mot de passe (contrôle)".

Suite à la saisie de ces informations contractuelles, il faut enregistrer l'établissement en cliquant sur le bouton <Appliquer>.



## 3.5 Initialisation

Si toutes les données contractuelles sont saisies et l'assistant fermé avec le bouton <Appliquer>, le bouton <Initialisation> apparaît dans le programme E511 "Configuration des établissements". En cliquant sur ce bouton, les lettres d'initialisation de ce contrat sont créées.



### Indication

Les deux lettres d'initialisation sont créées au format HTML, comme indiqué dans l'initialisation de la communication. Ces lettres sont enregistrées dans le répertoire suivant :

`\abac\kd\nrX\lepay\infiles\[numéro et désignation de l'établissement]\ini\[date]`

Les deux documents HTML doivent être imprimés, signés par la personne figurant dans le contrat et envoyés à l'établissement financier.



Ci-dessous un extrait du site Internet d'un établissement financier concernant le déroulement d'EBICS :

*Le participant transmet sa clé publique à l'établissement de crédit par deux voies de communication indépendantes l'une de l'autre :*

1. *La transmission des clés de participant publiques à l'établissement de crédit s'effectue en ligne par le type d'ordre INI (envoi de la clé publique bancaire) et le type d'ordre HIA (envoi de la clé d'authentification publique ainsi que de la clé de cryptage publique) et est définie en tant qu'initialisation du participant.  
(Remarque Abacus - advenu lors de l'initialisation)*
2. *En outre, le participant envoie par courrier postal la lettre d'initialisation signée pour activation et archivage à la banque.  
(Remarque Abacus - ce sont les deux documents HTML à imprimer)*



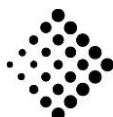
## Indication

Vous trouvez un exemple des lettres INI et HIA à la en page 17, resp. en page 18 de ce descriptif.

## 3.6 Validation des clés bancaires par l'établissement financier

Après l'initialisation, la signature et la transmission des documents à l'établissement financier, une communication n'est pas encore possible, car l'établissement financier doit d'abord vérifier les informations fournies et ensuite valider les clés bancaires. Cela peut prendre quelques jours de travail, selon l'établissement. Mais il faut au minimum prendre en considération la durée de l'acheminement postal et y ajouter un jour pour le traitement.

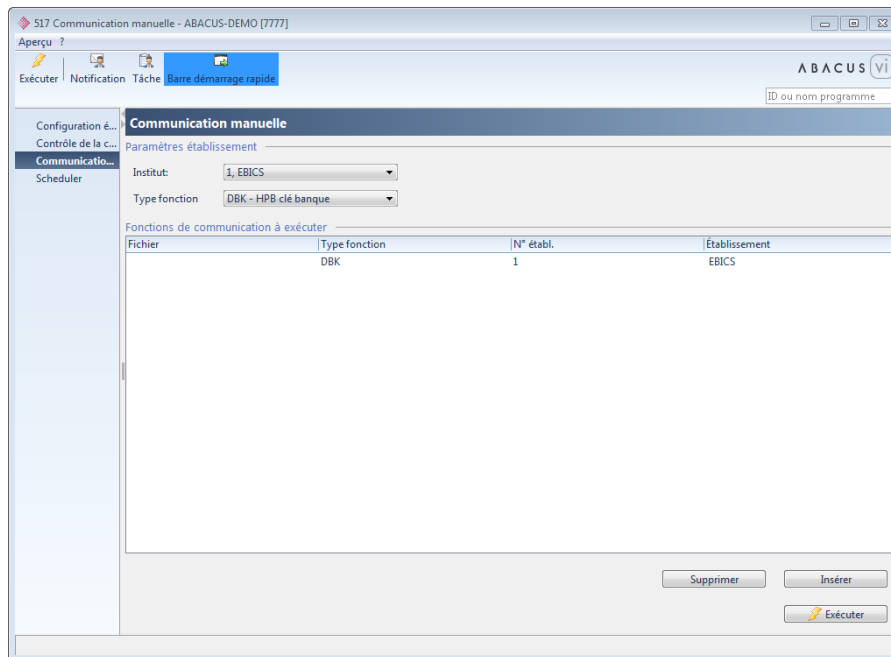
Chaque établissement gère différemment la validation des clés et l'information au client suite à la validation. Certains établissements informent par écrit ou par téléphone, d'autres n'informent pas du tout.



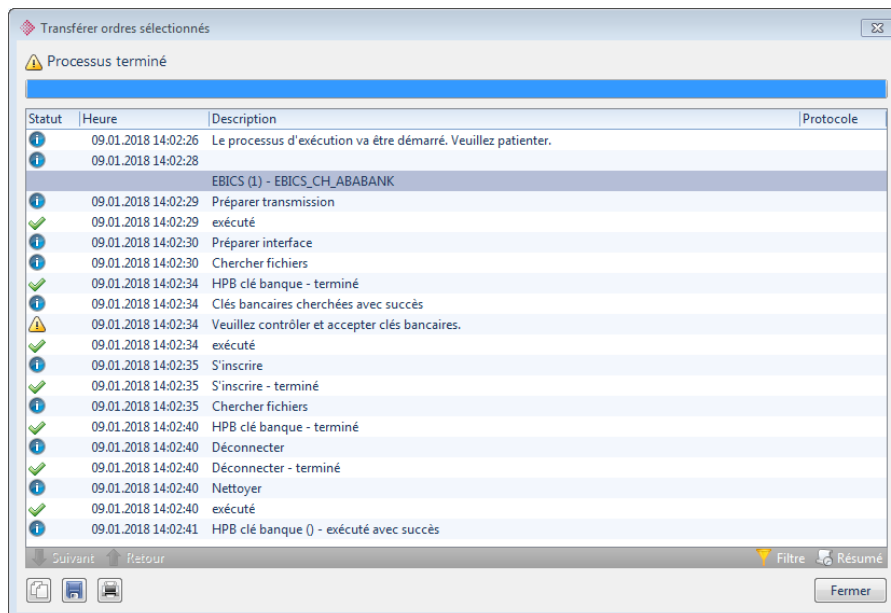
## 3.7 Chercher / télécharger les clés bancaires

Suite à l'information de l'établissement confirmant la validation des clés bancaires ou - si aucune réponse de l'établissement n'a suivi - au plus tôt après 2 à 3 jours, vous pouvez télécharger les clés bancaires.

Pour ce faire, vous sélectionnez l'établissement EBICS et le type de fonction "DBK - HPB Clé bancaire" ou "DBK - Download clé bancaire" dans le programme 517 "Communication manuelle", et cliquez ensuite sur le bouton <Ajouter> puis sur <Exécuter>.



Les clés bancaires activées se présentent comme suit :



Ce message apparaît si les clés bancaires ont été téléchargées avec succès. Celles-ci doivent maintenant être confirmées par l'administrateur dans le programme 511 "Configuration des établissements".





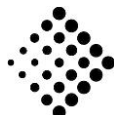
## Indication

Aucune donnée telle que les mouvement des comptes n'a encore été téléchargée. Tant que les clés bancaires n'ont pas été contrôlées et acceptées, il n'est toujours pas possible d'échanger des données avec l'établissement financier.

Si les clés bancaires ne sont pas encore à disposition, le message suivant apparaît :

*Le téléchargement des clés bancaires a échoué. Vous n'êtes probablement pas encore libéré par la banque. L'activation des clés bancaires peut prendre plusieurs jours. Réessayez plus tard. Aucune donnée n'a été cherchée ou transmise.*

Il faut attendre jusqu'à ce que les clés soient libérées par l'établissement. Veuillez s.v.p suivre la recommandation et réessayer le téléchargement des clés plus tard. Sinon veuillez contacter l'établissement.



## 3.8 Confirmation clé bancaire / accepter Hash

Afin de pouvoir confirmer les valeurs Hash, celles-ci doivent être comparées avec les valeurs du contrat bancaire.

Si les deux Hashes (1.) correspondent aux valeurs des documents du contrat, la case "Accepter Hash" (2.) peut être cochée et le paramètre sauvegardé en cliquant sur <Appliquer>.

The screenshot shows the 'Modifier établissement / contrat' window. The 'Clé du contrat' section contains the following data:

Fichier paramètres banque	EBICS_1
Libérer pour d'autres mandants	7777
	7777

The 'Détails contrat' section contains the following data:

Description	EBICS
IDClient	USER18
HostID	ABABANK
Adresse Internet	https://ebicsbank02.abacus.ch/ebics
Variante interface	EBICS_CH_ABABANK
Hash auth. banque	23491E04B348ADC22AA63B95648E8B1E8ABB90FCE187E3C69BAD2698FA470791
Hash crypt. banque	6281D8CFDEA1CF449EDDF14F59A489895B08F2764168E5771BBD89FEB610F4B0
Accepter Hash	<input checked="" type="checkbox"/>
UserID	USER18
Nom de l'utilisateur	Hans Muster
Mot de passe	...
Mot de passe (Contrôle)	...
Statut client à la banque	READY





## 3.9 Activer Recevoir types d'ordre et Envoyer types d'ordre

Tous les formats convenus avec l'établissement financier doivent être sélectionnés. Ces formats peuvent également être activés ou désactivés ultérieurement.

Si tous les paramètres sont effectués, vous les confirmez avec le bouton <Appliquer>.



### Information

EBICS est maintenant installé et toutes les données convenues par contrat avec l'établissement financier peuvent être échangées.



## 4 Annexe – Exemple de lettre INI

### Lettre d'initialisation pour clés électroniques bancaires

Nom d'utilisateur Hans Muster  
Date 01.01.2017  
Heure 12:00:00  
Destinataire BANQUEDÉMO  
*User-ID* USER1  
ID client Abacus1

Version UE A005

Clé publique (Public Key) pour la signature électronique :

Exposant 17

1 00 01

Modulo 1536

A2 6A CF 8C B3 DA 11 45 25 D6 1A 22 4B A6 7F 80 72 F9 1F B1 6B 8C 41 12  
7D F6 06 47 E0 28 08 AE E5 4B 11 02 5F C6 37 17 41 68 66 91 89 D2 C4 46  
FC 60 AA D3 F0 B8 DA 3D 6D 5E AE 92 10 20 22 58 C4 65 94 C7 C7 6D F1 33  
34 F9 91 5A F4 AE 27 70 D4 99 67 5F 5C 01 6D 77 1C 89 8E 23 2B 7E 1F 6C  
EX 18 6D 36 98 AE 22 EB F6 C9 A9 B9 64 C9 A8 87 40 F0 E1 F1 B2 CB 2B FE  
73 80 55 EA A8 E8 BB 50 38 AE 41 D9 1F 58 2E 58 C3 05 56 E2 2A 1A FD 81  
9A 63 44 04 1F 6B C8 11 28 B3 44 EB D9 6B EA 83 71 F8 A6 09 88 2A 7F 60  
43 AE 60 8F 11 BA 48 CB 1D 01 57 54 73 AB 57 43 47 22 44 39 C1 BC F5 C7

Hash SHA256

5B 69 78 74 96 E0 CB 89 E9 B3 19 B2 03 SA F8 70  
AC 56 45 55 16 D5 3E 6D 49 51 42 0E 90 8E 31 09

Je confirme par la présente la clé publique ci-dessus pour ma signature électronique.

---

Lieu / date

Entreprise / Nom

Signature



**5 Annexe – Exemple de lettre HIA****Lettre d'initialisation pour clés électroniques bancaires**

Nom d'utilisateur Hans Muster  
Date 01.01.2017  
Heure 12:00:00  
Destinataire BANQUEDÉMO  
User-ID USER1  
ID client Abacus1

Version signature d'authentification X002  
Version cryptage E002

Clé d'authentification publique :

Exposant 17

1 00 01

Modulo 1024

B9 0B C6 E8 0E BA C6 DA 2F 9E 74 AB 0F 08 59 5E 58 9F FC DE 11 01 AE 96  
1A 23 7F 31 C3 41 09 F1 49 ED 26 DE 77 A4 9E 6A AD 42 C5 94 9D CB 1B 2A  
68 DC F6 4C C3 SA 8F B4 2A 50 54 D5 4A E0 04 B2 28 63 5C C2 61 E6 47 11  
A0 C1 02 E0 08 2C 50 81 61 SA 93 63 B5 2A 7D 27 5D 32 F2 EX F3 99 B0 A5  
F0 7C 2F 56 FA 0C F7 D0 E5 A9 1D 9D 6C 02 6B E5 E3 A3 3F E4 FF 23 3A 7F  
41 70 3E 9B 98 31 83 E9

Hash SHA256

FC 73 C2 8D 1E C0 FD 96 F4 05 17 0F 1C 0A 72 36  
A0 A6 28 BF C2 D5 01 FA 45 B3 72 3A F9 2B 6E 55

Clé de cryptage publique :

Exposant 17

1 00 01

Modulo 1024

8F 9E FC 36 2C 72 C9 45 47 CB 6F 02 C6 7E 52 AE 57 95 36 AA 57 41 81 F4  
90 79 0B 63 88 B8 B9 52 31 60 6E 99 17 C9 C9 2D CE D0 AB A5 A2 A0 49 78  
EA 8F 94 BE 30 98 9C 23 C8 61 60 2A 03 43 9D 24 42 86 FE 85 74 F2 6A F2  
SA AA 2D 4A 81 03 9B E3 19 BF 26 E1 ED 82 80 83 58 4F 15 33 D0 1D C4 D4  
D4 BC B2 28 A5 C0 13 5B 0D F1 29 13 26 CC 6D F5 AB 8B 2B A9 70 A7 7B 4F  
C1 A2 46 0B 2E 0E 6D BF

Hash SHA256

60 5A FB A1 C6 2E 0F 06 A8 FB 21 7F 73 BF 10 38  
27 86 63 F6 31 14 F6 8A 7C 88 F8 E9 C5 91 18 5D

Je confirme par la présente les clés publiques ci-dessus.

\_\_\_\_\_  
Lieu / date

\_\_\_\_\_  
Signature

