

# A B A C U S DESCRIPTIF D'INSTALLATION

## **ELECTRONIC BANKING** **EBICS**

Dès version 2014 (avec patch du 20.01.2015)

**Février 2015 / mlu / 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) 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 © 2015 by ABACUS Research SA, CH-9301 Wittenbach-St.Gallen

<b>Avant l'installation.....</b>	<b>1</b>
Documents importants et interlocuteurs.....	1
Protocole soutenu .....	1
Restrictions d'ABACUS.....	1
Mise à jour EGI .....	2
Paramètres de communication .....	3
<b>Installer EBICS.....</b>	<b>5</b>
1. Choix du serveur de communication et du proxy .....	5
2. Sélection établissement .....	6
3. Attribution du contrat.....	7
4. Définition du contrat .....	8
5. Initialisation .....	9
6. Chercher/télécharger les clés bancaires.....	11
7. Confirmation clés bancaires/Hash .....	13
<b>Annexe – Exemple de lettre INI .....</b>	<b>14</b>
<b>Annexe – Exemple de lettre HIA.....</b>	<b>15</b>

# 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.
- ✓ La personne responsable, qui connaît le mot de passe administrateur d'ABACUS, ainsi que le responsable du réseau devraient au moins être joignables.



### Sécurité

Le programme Electronic Banking d'ABACUS vous propose une multitude de mesures de sécurité comme le cryptage des données sensibles, la demande du mot de passe, la règle des signatures, etc.



### Attention

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

## 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

## Restrictions d'ABACUS

- La signature distribuée 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.

## Mise à jour EGI

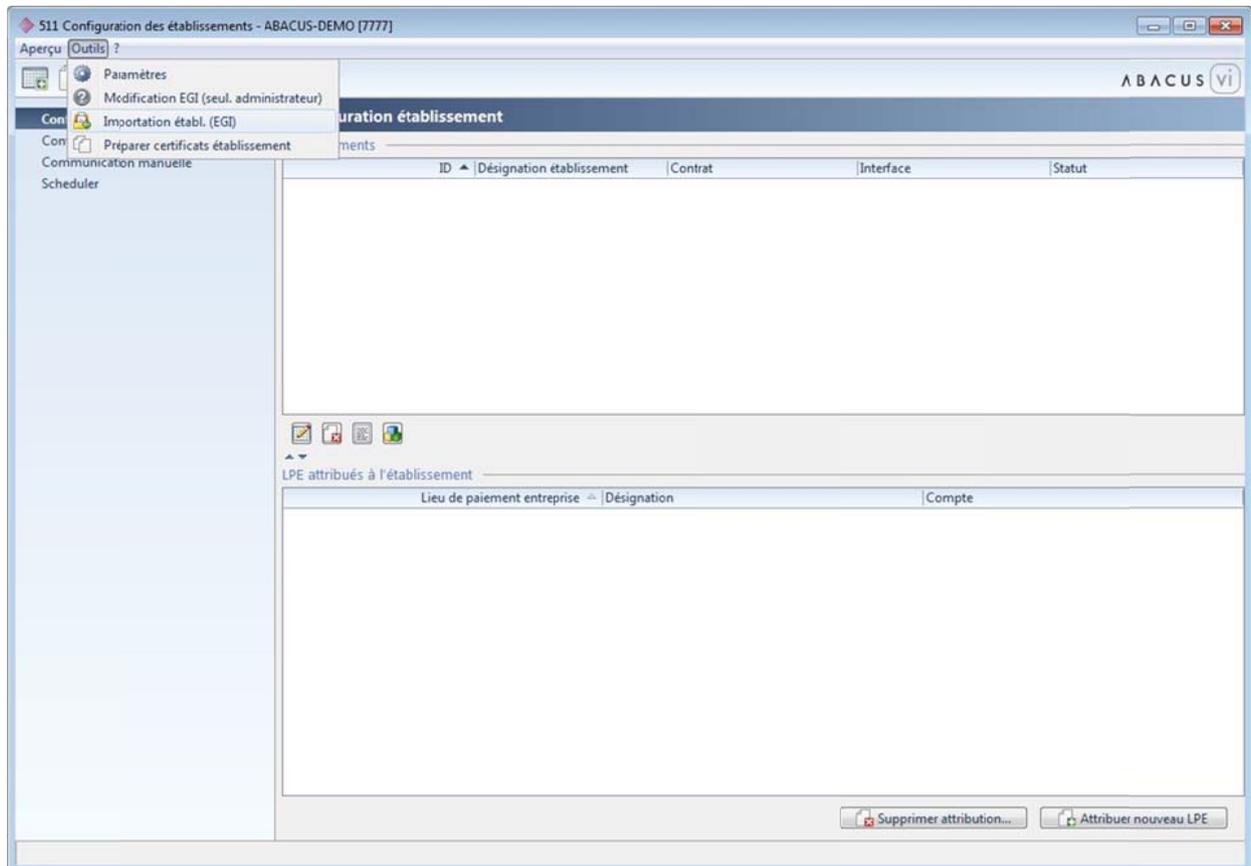
Avec la mise à jour EGI, d'éventuelles modifications des interfaces bancaires peuvent être importées dans ABACUS, indépendamment des mises à jour et des installations patch. Une mise à jour est toujours judicieuse si un nouvel établissement est configuré. Les établissements existants n'en sont pas influencés.

L'actuel fichier EGI est mis à disposition par ABACUS sous le lien suivant :

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

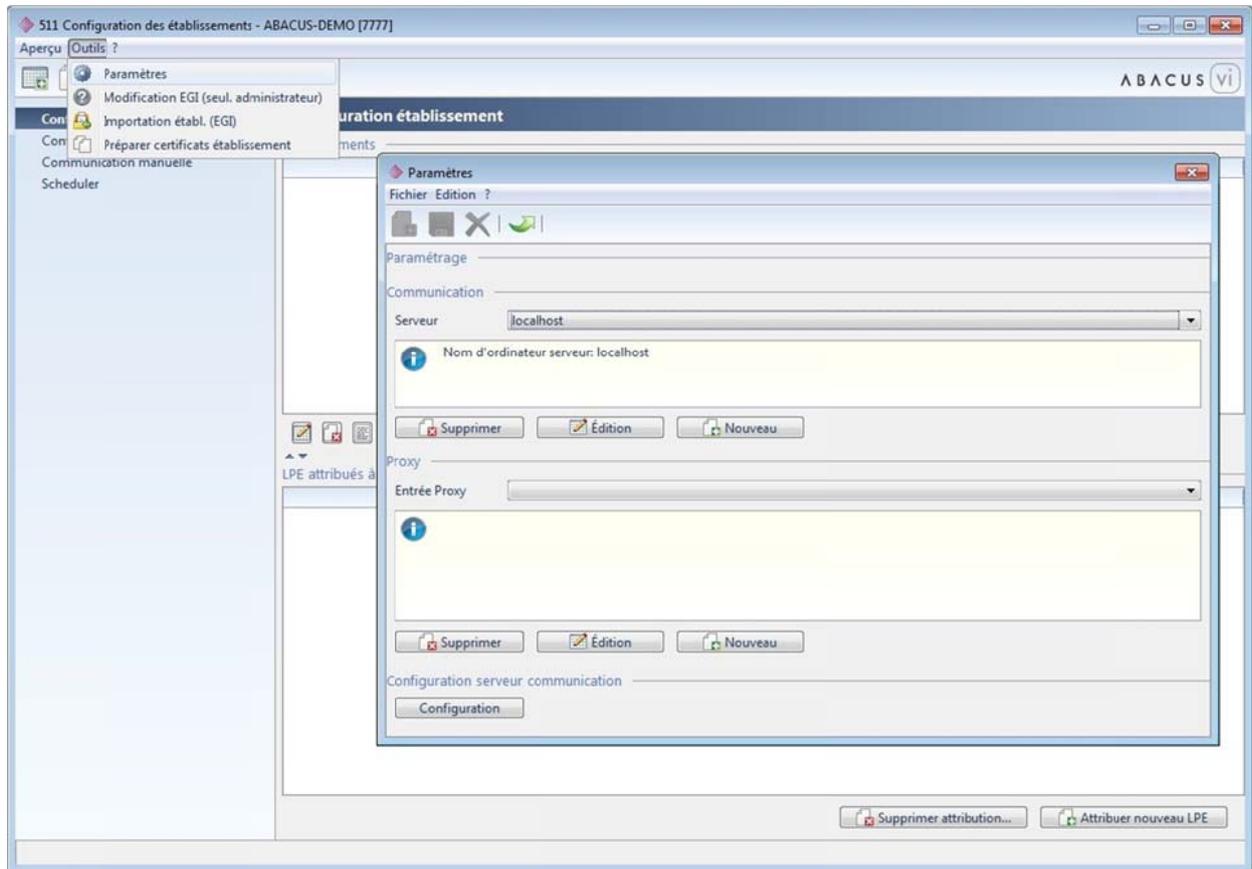
Nom du fichier	Taille	Date de création
Installation instituts financiers V2011 / 2012 (PDF)	5 MB	21.02.2014
Liste des établissements bancaires (HTML)	56 Kbyte	02.11.2015
Update EGI (ZIP)	9 Kbyte	02.11.2015

La fonction "Importation établ. (EGI)" du programme E511 Configuration des établissements permet d'importer dans l'Electronic Banking le XML extrait du fichier ZIP.



## Paramètres de communication

Les paramètres de communication doivent être indiqués avant la configuration des établissements.

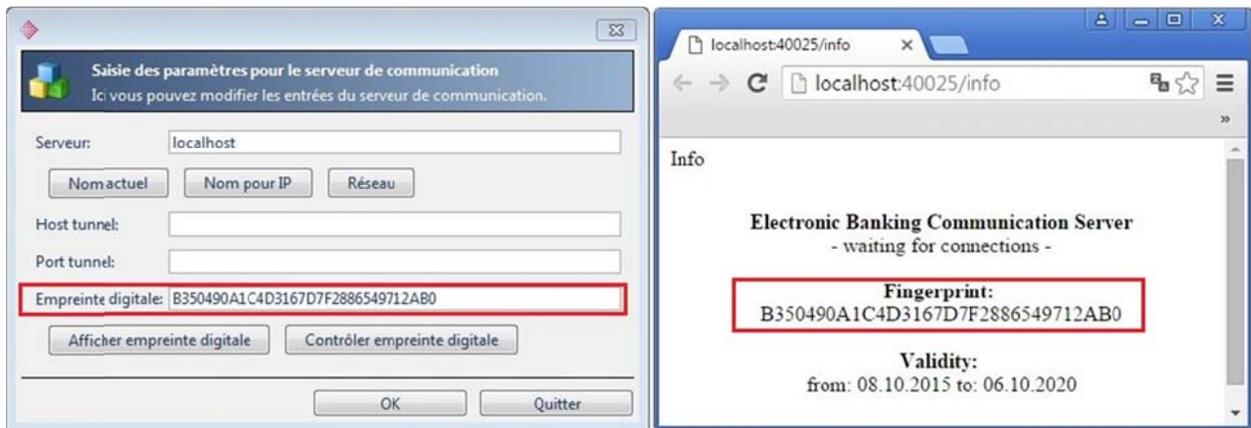


Ces paramètres sont ouverts sous "Outils - Paramètres" dans le programme 511.

### Serveur de communication

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".

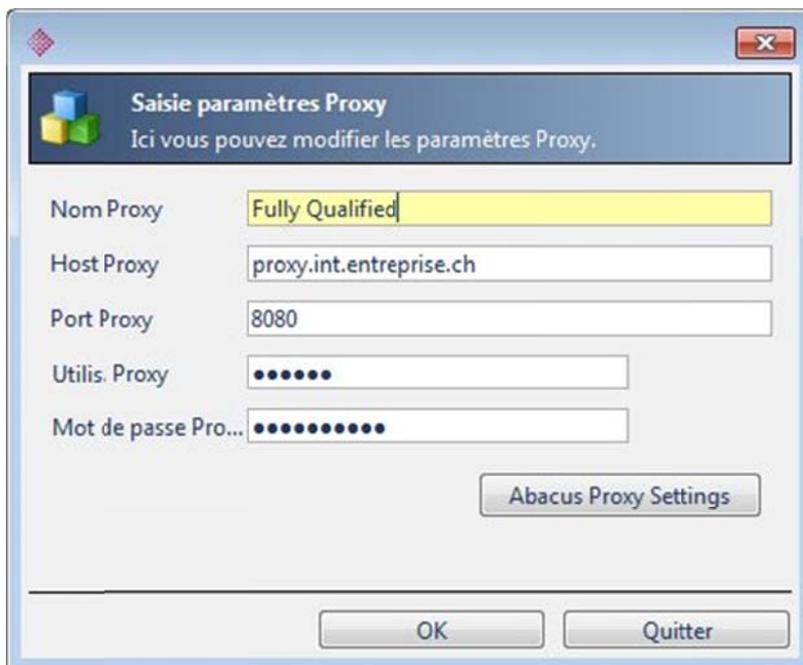
Normalement, le nom du serveur de communication correspond à l'ordinateur sur lequel ABACUS est installé. Dans ce cas, cliquez sur le bouton "Nom actuel". Si le serveur n'est pas trouvé grâce au nom (DNS), le bouton "Nom pour IP" permet de déterminer son adresse IP. Si la communication se fait au moyen 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.



Chaque entrée de serveur exige l'indication d'une empreinte digitale (fingerprint). Celle-ci est générée par le bouton "Afficher Fingerprint" et affichée dans une fenêtre du navigateur (par ex. Internet Explorer ou Firefox). Cette valeur est à copier et à insérer dans le champ correspondant. En cliquant ensuite sur le bouton "Contrôler Fingerprint" vous vérifiez si l'empreinte digitale est correcte.

## Proxy

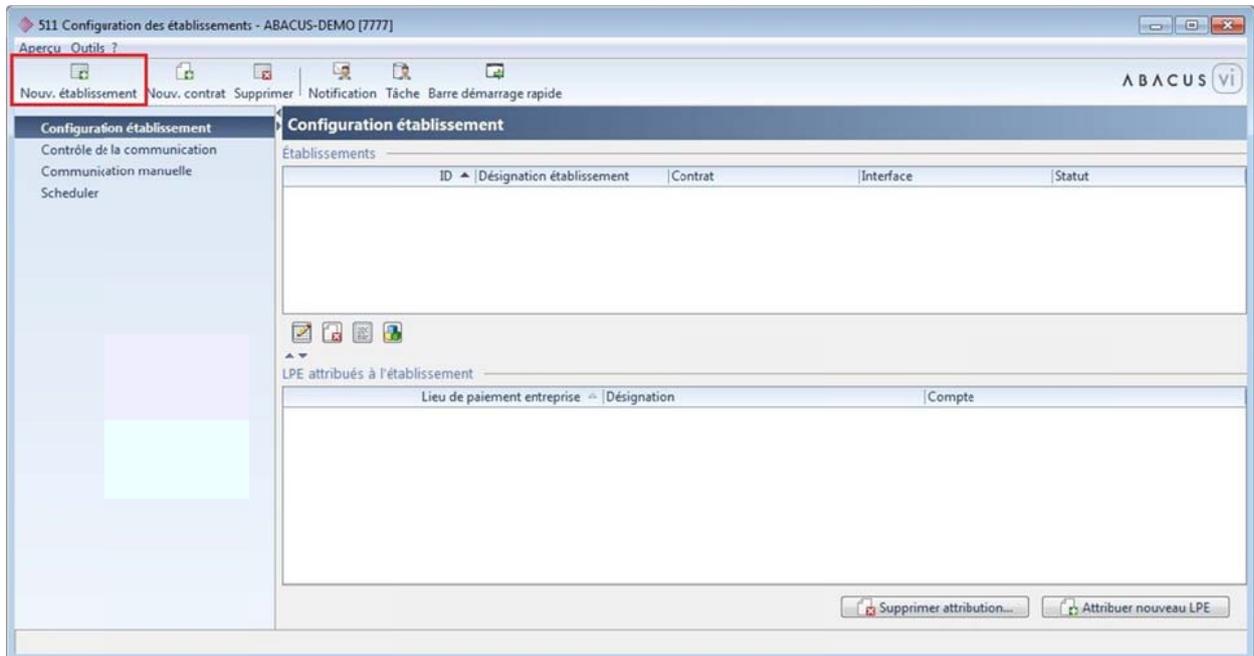
Si un serveur Proxy est utilisé pour la communication depuis le réseau de l'entreprise vers l'internet, les paramètres correspondants peuvent être enregistrés sous "Proxy". Le bouton "Nouveau" permet de créer un nouvel enregistrement et le bouton "Édition" de le modifier. Si une entrée Proxy existante n'est plus utilisée, vous pouvez la sélectionner puis la retirer avec "Supprimer".



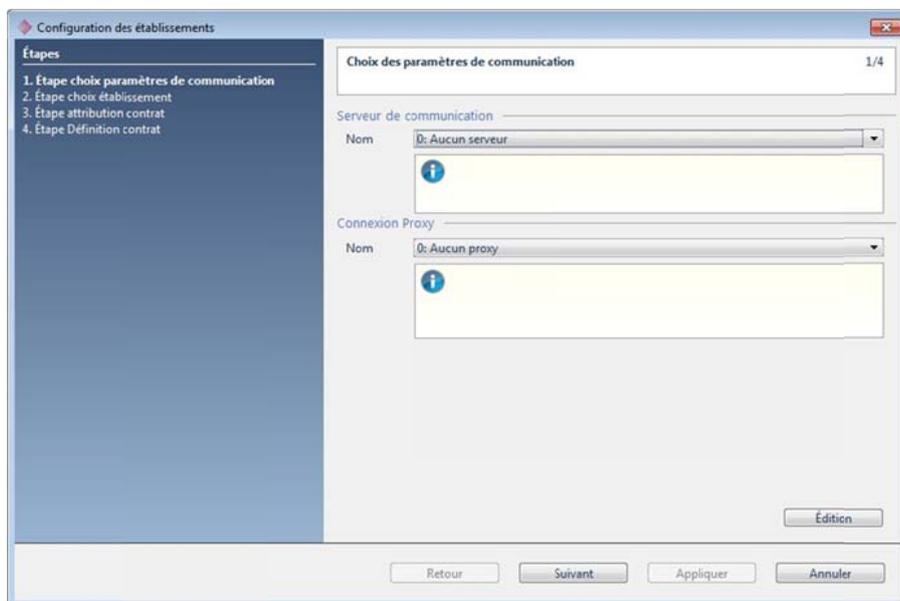
Les préparations pour l'installation d'un établissement avec EBICS sont terminées. Le processus de configuration de l'établissement est décrit dans les pages suivantes.

# Installer EBICS

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



## 1. Choix du serveur de communication et du proxy



Ici vous pouvez sélectionner le serveur de communication et l'éventuelle entrée proxy. Si nécessaire, vous pouvez créer ou modifier ces paramètres à l'aide du bouton "Édition" (voir chapitre Paramètres de communication pages 3/4).

## 2. Sélection établissement

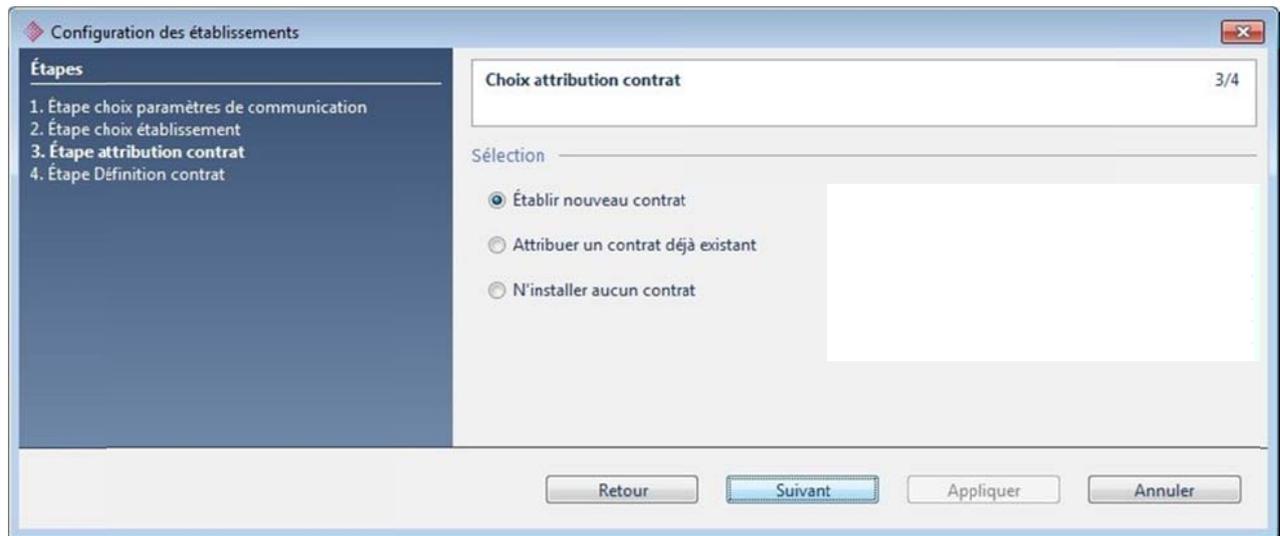
The screenshot shows a software window titled 'Configuration des établissements' with a sub-header 'Choix établissement' and a progress indicator '2/4'. On the left, a sidebar lists four steps: 1. Étape choix paramètres de communication, 2. Étape choix établissement (highlighted), 3. Étape attribution contrat, and 4. Étape Définition contrat. The main area is titled 'Groupe établ.' and contains the following fields: 'Établ. financier' (a spinner box set to '2' with a dropdown arrow and 'EBICS' text), 'Pays' (a dropdown menu set to 'CH'), another 'Pays' dropdown menu set to 'Standard', 'Désignation' (a text box containing 'EBICS'), 'Interface' (a dropdown menu set to 'EBICS'), 'Mot de passe' (an empty text box), 'Contrôle mot de ...' (an empty text box), 'Statut' (a dropdown menu set to 'Installer'), and 'N° Intercompany' (a text box containing '0'). At the bottom, there is a checkbox labeled 'Avis de débit global SEPA' which is checked. At the very bottom of the window are four buttons: 'Retour', 'Suivant', 'Appliquer', and 'Annuler'.



### Description des champs

Établissement financier	Choisir l'établissement financier 2 "EBICS".
Désignation	Le choix de la désignation est libre. Il est important, avec plusieurs établissements, de choisir des désignations explicites afin de les discerner ultérieurement les uns des autres.
Interface	ABACUS reconnaît automatiquement l'interface en fonction de l'établissement financier choisi.
Statut	Le statut "Installer" doit rester. Il passe automatiquement à "En service" une fois l'installation terminée.
Avis de débit global SEPA	La case pour cet avis est cochée par défaut. La plupart des établissements financiers attendent les versements par ordre de paiements collectif. Si vous avez convenu avec l'établissement des paiements individuels, vous devez supprimer la coche.

### 3. Attribution du contrat



#### Description des champs

Établir un nouveau contrat	Pour installer un nouveau contrat, si celui-ci n'existe pas déjà dans un autre mandant, vous pouvez choisir ici (par défaut).
Attribuer un contrat déjà existant	Sélectionnez ce point si le contrat a déjà été importé (contrats communs aux mandants, établissement supprimé) et si vous désirez ouvrir à nouveau un établissement financier.
N'installer aucun contrat	Un établissement est créé sans contrat. Une communication en ligne n'est pas possible par la suite.

## 4. Définition du contrat

The screenshot shows a software window titled 'Configuration des établissements' with a sub-tab 'Définition contrat' (4/4). On the left, a sidebar lists four steps: 1. Étape choix paramètres de communication, 2. Étape choix établissement, 3. Étape attribution contrat, and 4. Étape Définition contrat. The main area is divided into two sections: 'Clé du contrat' and 'Détails contrat'. 'Clé du contrat' includes a dropdown for 'Fichier paramètres banque' (set to 'EBICS\_1') and a text field for 'Libérer pour d'autres mandants' (set to '[Aucun(e)]'). 'Détails contrat' contains several fields: 'Description' ([NomBanque] EBICS), 'IDClient' (ABACUS1), 'HostID' (BANQUEDEMO), 'Adresse Internet' (https://banquedemo.institut.ch/ebics), 'UserID' (USER1), 'Nom de l'utilisateur' (Fernand Dell), 'Mot de passe' (masked with dots), 'Mot de passe (Contrôle)' (masked with dots), 'Variante interface' (empty), 'Hash auth. banque' (empty), 'Hash crypt. banque' (empty), an unchecked checkbox for 'Accepter Hash', 'Statut client à la banque' (NEW), and a checked checkbox for 'Download extraits de compte MT940'. At the bottom, there are four buttons: 'Retour', 'Suivant', 'Appliquer', and 'Annuler'.



### Descriptions des champs

#### **Description:**

Désignation librement définissable pour le contrat.

#### **HostID:**

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

#### **UserID:**

ID utilisateur selon les documents du contrat.

#### **Mot de passe:**

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

#### **Cases formats**

Pour télécharger les clés bancaires, la case "Télécharger extraits de compte MT940" doit être cochée. Après avoir cherché et accepté les clés bancaires (voir "7 Confirmation clés bancaires/Hash" à la page 13), vous pouvez si nécessaire supprimer cette coche.

#### **IDClient:**

ID client selon les documents du contrat.

#### **Adresse Internet:**

URL de l'établissement selon les documents du contrat.

#### **Nom d'utilisateur:**

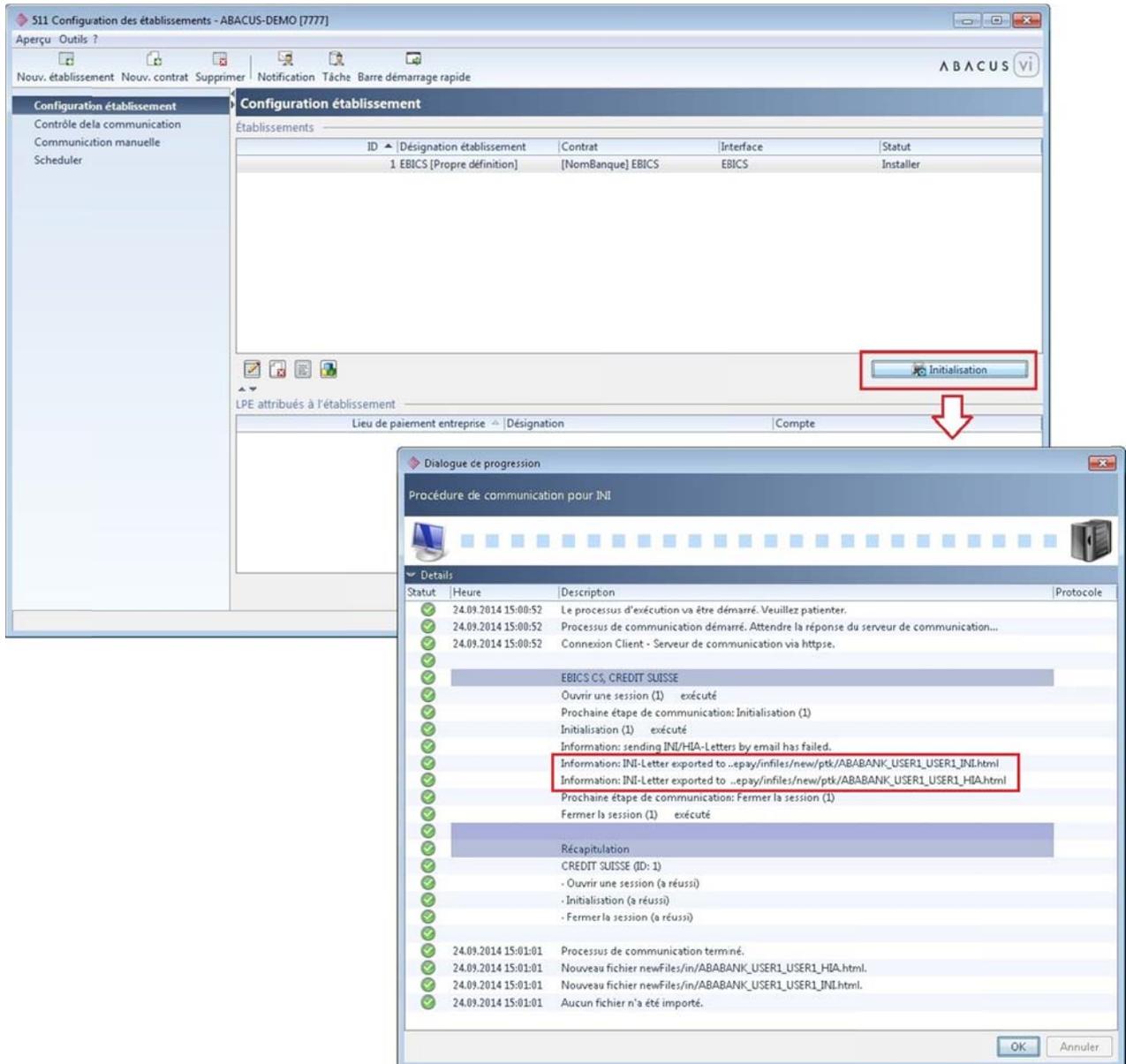
Prénom et nom de la personne figurant dans le contrat EBICS.

#### **Statut client à la banque:**

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

## 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. En cliquant sur ce bouton, les lettres d'initialisation de ce contrat sont créées.



### Indication

Comme décrit dans la procédure de communication de l'initialisation, les deux lettres d'initialisation sont exportées en format HTML vers le répertoire X:\abac\kd\nrX\epay\infiles\new\ptk. 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 aux pages 14 et 15 de ce descriptif.

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

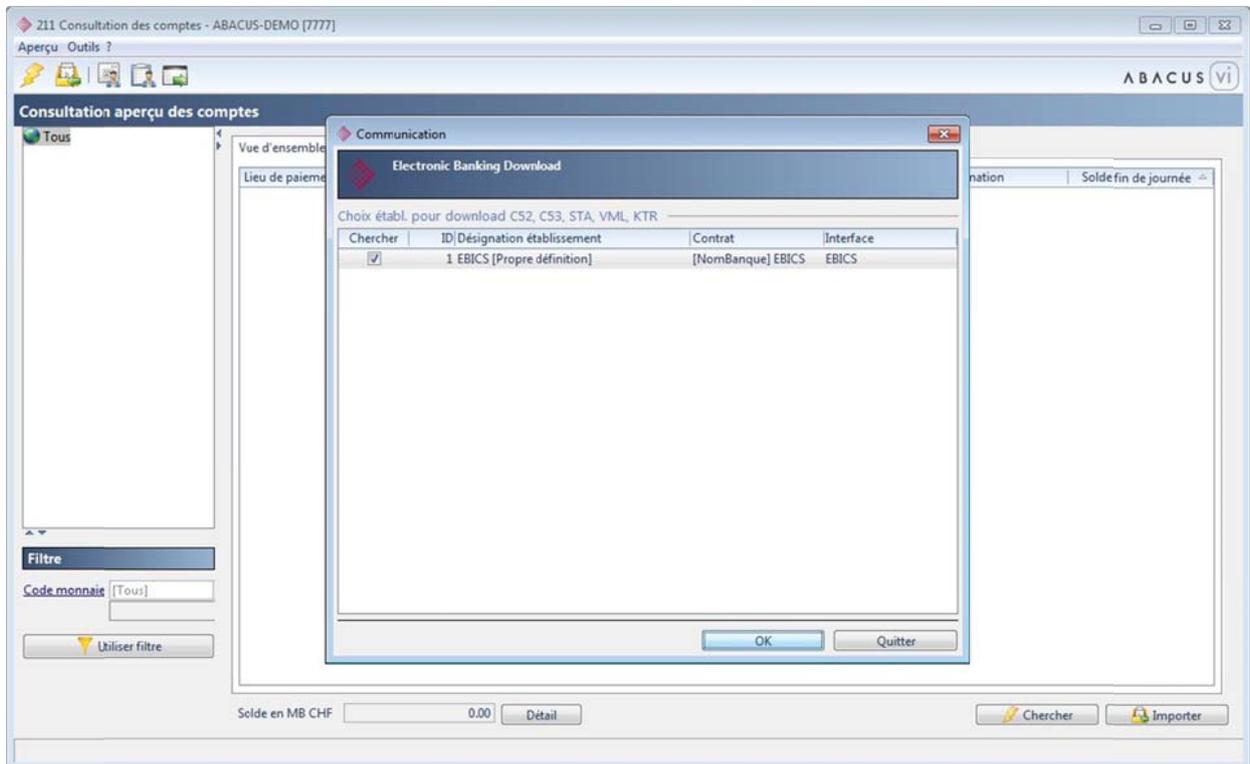
Après l'initialisation, la signature et la transmission des documents, il n'est pas encore possible de communiquer avec l'établissement, car celui-ci doit d'abord vérifier les informations fournies et ensuite valider les clés bancaires. Cela peut prendre plus ou moins de temps, selon la banque. Mais 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 envoient une lettre et d'autres n'informent pas du tout.

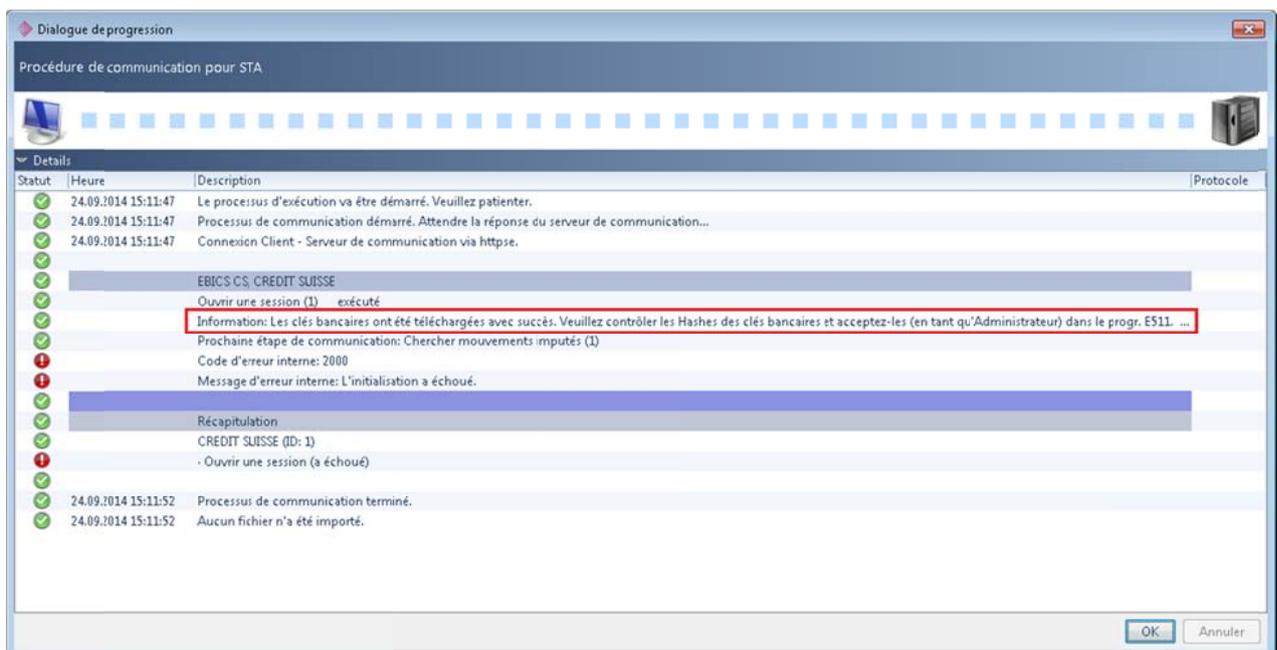
## 6. Chercher/télécharger les clés bancaires

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

Dans le programme E211 Consultation aperçu des comptes, vous cliquez sur le bouton "Chercher", vous choisissez l'établissement EBICS et vous lancez la communication.



Les clés bancaires activées se présentent comme suit:



**Information:** Les clés bancaires ont été téléchargées avec succès. Veuillez contrôler les Hashes des clés bancaires et les accepter (en tant qu'Administrateur) dans le progr. E511. Les données ne pourront être transmises ou cherchées que suite à ce pas.

Les clés bancaires ont été téléchargées avec succès et doivent être confirmées par l'administrateur dans le programme E511.



### **Indication**

Aucune donnée de compte n'a encore été saisie. 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 plus tard. Sinon veuillez contacter l'établissement.

## 7. Confirmation clés bancaires/Hash

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

Si les deux hashes correspondent aux valeurs des documents du contrat, la case "Accepter Hash" peut être cochée.

Ensuite il faut sélectionner les formats convenus avec l'établissement. Ces formats peuvent également être activés ou désactivés ultérieurement.

Détails contrat

Chemin Ciphering Softcert	
Mot de passe Ciphering Softcert	••••••
Mot de passe Ciphering Softcert (Contrôle)	••••••
Nom certificat Ciphering (alias)	
Hash auth. banque	6ED5E22C3EA95C492845586FC935C33333F468A2F931C8B443D516E1E7844CD5
Hash crypt. banque	5F07D7598B1146B5A0C99CC67B0B7254308587B4C18DCF40E3C0FB7B7B2E52FD
<input checked="" type="checkbox"/> Accepter Hash	←
Statut client à la banque	READY
<input checked="" type="checkbox"/> Download extraits de compte MT940	

Annuler Appliquer

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



### Important

Les informations concernant les divers formats sont disponibles chez l'établissement correspondant ou sur le site Internet [www.iso20022.ch](http://www.iso20022.ch).

Concernant la migration du trafic des paiements suisse, veuillez consulter l'article de ABACUS Pages 2/2014

([http://www.abacus.ch/fileadmin/mediendatenbank/kundenmagazin\\_fr/2014\\_fr/2/s09-14\\_fr.pdf](http://www.abacus.ch/fileadmin/mediendatenbank/kundenmagazin_fr/2014_fr/2/s09-14_fr.pdf)) ou la page Web citée ci-dessus.



### Information

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

# Annexe – Exemple de lettre INI

## Lettre d'initialisation pour clés électroniques bancaires

Nom d'utilisateur Jean Démo  
Date 01.01.2015  
Heure 12:00:00  
Destinataire BANQUEDÉMO  
User-ID USER1  
ID Client ABACUS1

Version EU 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 AF 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 EE 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 EE 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 EA 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.

\_\_\_\_\_  
Entreprise/nom

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

Signature : \_\_\_\_\_

# Annexe – Exemple de lettre HIA

## Lettre d'initialisation pour clés électroniques bancaires

Nom d'utilisateur Jean Démo  
Date 01.01.2015  
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 EA 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 EA 93 63 B5 2A 7D 27 5D 32 F2 AF 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  
EE 8F 94 BE 30 98 9C 23 C8 61 60 2A 03 43 9D 24 42 86 FE 85 74 F2 6A F2  
EA 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