

Point de vue : centraliser soit, mais rationaliser d'abord !

par Eric Gayno,
UTSIT

Les grands projets de centralisation de la communication bancaire peuvent vite tourner au casse-tête et à l'embolie administrative si les contrats et pouvoirs de signature bancaire ne sont pas adaptés à cette organisation.

Bonne nouvelle, la solution de signature multi-bancaire et multi-pays est enfin disponible. Avec l'avènement de 3SKey, le canal de communication bancaire qui permet de parler quasiment à toutes les banques est utilement complété d'une solution de signature couvrant potentiellement le même périmètre de banques. Beaucoup d'entreprises qui ont lancé des projets de communication bancaire « groupe » souhaitent atteindre deux objectifs qui peuvent s'avérer très contradictoires. Le premier est de centraliser la relation administrative avec les banques voire les groupes bancaires. Le second est de conserver la responsabilité de signature dans les filiales.

Deux écueils

La plupart des grandes entreprises a des règles de signature des ordres de paiement laissées à l'initiative de chacune des filiales qui définit ses collèges et ses plafonds. Même quand des règles « groupe » existent, leur application locale donne lieu à une nécessaire adaptation au terrain. De ce fait, vouloir faire rentrer dans une même matrice ces différentes règles peut s'avérer très complexe. Mais pire encore, demander à la banque de vouloir contrôler ces différentes règles peut s'avérer tout simplement impossible. En effet, à un même contrat de communication bancaire on peut généralement associer un et un seul jeu de règles, ce qui interdit donc d'imaginer de demander à la banque de contrôler à la fois la combinatoire collèges/plafonds de la filiale A et celle différente de la filia-

le B. On sera donc bien avisé de commencer par harmoniser de manière drastique les règles des pouvoirs bancaires.

A ce premier écueil il faut en ajouter un deuxième, lié au nombre de signataires et au renouvellement des listes. Très souvent chaque filiale a une relation avec une agence et les pouvoirs bancaires sont donc assez simples, les listes courtes et les renouvellements peu fréquents. Mais tout agrégé on peut rapidement se retrouver avec des listes longues et des renouvellements plus complexes à gérer. Sans parler de la logistique centralisée de distribution des dispositifs de signature et leur renouvellement en catastrophe en cas de perte ou de détérioration.

Une question d'organisation s'impose alors : ne faut-il pas, à l'occasion de la centralisation, réduire drastiquement le nombre de signataires et les loger dans l'entité centralisatrice ?

S'organiser autrement

A l'occasion des projets de centralisation, la sécurisation des échanges de fichiers entre les filiales et l'entité centralisatrice a toujours été considérée comme prioritaire. A juste titre. Très souvent la cinématique de validation fait intervenir les personnes en filiale dans le logiciel de communication bancaire hébergé et géré par l'entité centrale. Mais est-il pour autant nécessaire de transmettre leur action

à la banque sous forme de signature ? Beaucoup d'entreprises ont pensé que non et ont donc réservé un niveau de signature « interne » à ces signataires en filiale. Elles ont réservé la signature « externe », celle qui est transmise à la banque, à un petit groupe de personnes travaillant dans l'entité centralisatrice, celle qui a la relation au quotidien avec les services cash management des banques du groupe et qui gère les échanges de fichiers.

Bien entendu cette signature « interne » est tracée dans la piste d'audit et c'est souhaitable, les signataires internes utilisent des dispositifs de signature (clé USB, carte à mémoire) en tous points conformes à ceux qu'utilisent les signataires externes. A un détail près : les signatures restent sur place et ne vont pas à la banque.

Dans cette organisation les filiales ont donc donné un pouvoir spécial de signature des ordres télétransmis stipulant que les ordres transmis via SWIFTNet FileAct par l'entité centrale et signés par les signataires de la liste « Signataires de l'entité centrale » devaient être exécutés. Ce faisant, le groupe est organisé pour échanger simplement des listes de signataires courtes avec ses banques et pour gérer un parc restreint de dispositifs localisés au même endroit. ■



Edith Andreotta
© VIRBAC - All rights reserved.

Signer, mais pour quoi faire ?

par Loïc Colcomb,
UTSIT

La signature électronique des ordres de paiement présente des caractéristiques qui la différencient fortement de la signature des ordres papiers. La liste des signataires et leur rôle doivent sans doute être repensés à l'occasion de la mise en place de solutions dématérialisées.

Nombre de trésoriers l'avouent : ils ne regardent pas le détail des remises d'ordres qu'ils signent dans leur logiciel de communication bancaire. Parce que les informations proposées sont peu compréhensibles, parce que le nombre de « clics » à réaliser rend l'opération fastidieuse, parce que de toutes les manières ils ne savent pas donner un avis sur l'opportunité du paiement. Très souvent en effet, l'établissement de la liste des signataires électroniques s'est fait par simple transposition de la liste des signataires des ordres papier. Or le rôle des uns et des autres est bien différent, tant le processus du paiement lui-même est différent.

Un fichier contrôlé, verrouillé et documenté

Dans une entreprise bien organisée, comme le sont toutes celles que nous rencontrons, les ordres de paiement arrivent dans le logiciel de communication bancaire après tout un circuit de validation dans le progiciel de comptabilité fournisseurs. Saisie des coordonnées bancaires des fournisseurs, contrôle et saisie des factures, bon à payer, campagnes de règlement sont autant d'étapes pour lesquelles les notions de « ségrégation des tâches » et « principe des quatre yeux » ont été appliquées.

Le service informatique étant lui aussi bien organisé, les fichiers de paiement issus du progiciel de comptabilité en fin de processus sont écrits dans un répertoire auquel peu d'utilisateurs ont accès. De plus ils sont scellés et signés à l'aide d'un algorithme tel que PGP. Cette solution permet de s'assurer que seul le logiciel de communication bancaire pourra desceller les fichiers et garantit donc leur intégrité. Nul ne peut les modifier. Dans le logiciel de communication, aucune possibilité de modification des ordres importés n'est attribuée à qui que ce soit. Tout au plus est-il possible de rejeter un fichier, une remise, ou un ordre.

Dans cette entreprise modèle le service informatique a développé une enveloppe d'accompagnement de chaque fichier de paiement. Sur cette enveloppe sont indiquées des informations qui ne seront pas transmises à la banque mais qui sont utiles pour assurer la traçabilité de la chaîne. Le logiciel de communication bancaire, un des meilleurs du marché sans doute, sait interpréter les éléments de cette enveloppe et les inscrire dans sa « piste d'audit ».

Auditeur plus que signataire

De ce fait les deux signataires ont un rôle bien particulier : ils doivent être les « auditeurs » de tout ce qui s'est déroulé auparavant. Le rôle ne consiste plus à valider les factures une à une, pièces à l'appui, mais à utiliser leur connaissance des flux et des



métiers de l'entreprise pour jouer la fonction de « dernier rempart avant sortie des fonds ».

Dans la rédaction de la procédure interne décrivant le rôle de ces signataires et les critères qui ont amené à les désigner, on trouvera donc la définition de ce que l'on appelle un auditeur : quelqu'un qui est très à l'aise avec le fonctionnement de l'informatique en général et du logiciel de signature en particulier,

qui a une bonne connaissance des paiements habituellement effectués, des fournisseurs usuels, des pays de destination des fonds et des montants transférés dans les différentes devises. Ainsi il pourra jouer son rôle en utilisant sa connaissance de l'entreprise et en effectuant des sondages. A l'aide de la piste d'audit il peut demander à se faire communiquer une facture, ou bien aller jeter un œil dans le logiciel de comptabilité pour voir « qui a fait quoi ».

Enfin, mais ce n'est pas négligeable, cette fonction de signature peut s'avérer utile pour « prendre la température » des équipes en charge des campagnes de règlement, poser quelques questions sur les difficultés ou les joies du moment. En effet, très souvent, la signature se fait sur des postes spéciaux localisés dans les locaux de ces équipes. Aussi lorsque notre signataire/auditeur est un cadre de direction cette dernière fonction est-elle sans doute l'une des plus importantes. C'est pourquoi il faut faire signer régulièrement les signataires occasionnels que sont les directeurs.

«dernier rempart avant sortie des fonds»

Toute cette procédure ne vaut évidemment que pour les ordres de masse issus des applications de règlements fournisseurs. Les ordres saisis directement dans les logiciels de communication bancaire doivent être régis par une procédure toute autre et plus proche de la signature des ordres papier, et imaginer avoir des signataires différents est sans doute une très bonne idée. ■

3 SKey : du pilote à l'adoption

par Vianney Postic

Au début des années 90, Etebac-5 est déployé et les entreprises découvrent la signature personnelle, un outil qu'elles sont depuis quelques milliers à utiliser. Ce protocole est devenu obsolète et a été remplacé par SWIFTNet et, plus localement, EBICS. Les banques ont cherché une solution plus globale qu'Etebac pour répondre aux besoins de conformité, de sécurité et de standardisation des entreprises, et ont donc milité pour que Swift devienne une autorité de certification délivrant un certificat électronique permettant de signer des données échangeables, y compris éventuellement en-dehors du réseau SWIFTNet.

La sécurité peut être perçue comme une contrainte mais elle est un compromis permanent entre une – indispensable – politique sécuritaire drastique et son application quotidienne, avec toutes les contraintes que cela peut impliquer à un niveau local ou global. La clé du succès est donc l'adaptation permanente du niveau de sécurité à la situation, avec les risques encourus et calculés.

Pour mémoire, la sécurité des solutions de communication bancaire est un élément essentiel dans les relations banque-entreprise. Les quatre critères garants de la sécurité sont :

- L'authentification : s'assurer que notre interlocuteur est bien celui que l'on croit être.
- L'intégrité : s'assurer que la donnée n'est pas modifiée ou altérée.
- La confidentialité : s'assurer qu'un tiers ne peut comprendre la donnée échangée.
- La non-répudiation : mettre en place un système attestant de manière incontestable de la réalité de l'échange.

La combinaison de ces quatre critères permet d'obtenir la sécurité maximale. Le niveau de sécurité appelé « signature électronique » ou « signature personnelle » remplit les quatre critères mentionnés précédemment. Cette signature permet l'authentification nominative de l'utilisateur ayant signé le fichier transmis.

C'est ce qu'offre la nouvelle solution de SWIFT, la SWIFT Secure Signature Key, ou plus sobrement 3SKey. Elle a pour but d'étendre les fonctions et la souplesse d'Etebac-5 au monde entier en la combinant avec les normes draconiennes de sécurité établies par SWIFT. « Elle repose

sur trois idées simples, qui viennent s'ajouter aux composantes indispensables de la signature personnelle : une utilisation des meilleurs standards du moment, une simplicité accrue pour le client et une diminution des coûts d'intégration » dit Christian Durnez, SWIFT.

Une phase pilote a eu lieu en France l'été 2010, réunissant une vingtaine d'acteurs du marché : entreprises, éditeurs et banques afin de valider la solution. Elle a permis d'amener des améliorations immédiates, comme le souligne Anne-Françoise Coppola, de la Société Générale : « Certaines entreprises ont demandé la création de tokens administrateurs pour pouvoir gérer au mieux l'administration de tous les utilisateurs. Cette fonction a été intégrée dans le produit final, accroissant ainsi la sécurité de la solution ».

D'après Imad Ben Mariem, DataLog Finance, un certain nombre d'entreprises refusaient de migrer vers SwiftNet à cause du manque de réelle offre de signature personnelle ». Cette phase pilote a permis de comprendre leurs attentes et de calibrer la solution pour permettre de mieux y répondre. Certaines autres étaient confrontées à un problème lié au monde SaaS : « le transit sécurisé de très importants volumes de données entraînait une surconsommation inutile de temps et d'argent qui aurait pu être évitée. Plutôt que de transférer tout le fichier d'un poste à l'autre, Swift propose désormais au sein de 3SKey une clé d'identification chiffrée qui permet au destinataire de s'authentifier et de contrôler la validité de son fichier sans s'empêtrer dans une masse de processus et de données superflues ». explique Cyril Fandard, Kyriba.

“ Elle a pour but d'étendre les fonctions et la souplesse d'Etebac-5 au monde entier en la combinant avec les normes draconiennes de sécurité établies par SWIFT. ”

Suite au succès de cette phase, le produit a été lancé au SIBOS 2010 à Amsterdam et est en cours de déploiement. Si la France a été le premier pays à l'utiliser, il apporte l'énorme avantage de se placer dès son lancement dans un contexte international. François-Xavier Nivoit, HSBC, nous rappelle que « même si l'entreprise n'a pas à ce jour d'activité multinationale, 3SKey est pensé pour répondre à ses développements futurs et, à quelques mois seulement de la fermeture définitive du réseau X25, devient peu à peu de plus en plus indispensable dans notre environnement bancaire, s'imposant comme la solution pour répondre à l'avenir immédiat de la signature personnelle ». ■