IFCC
Institut de Formation de la Chambre de Commerce

a·t·e·l
Association des Trésoriers d'Entreprise à Luxembourg

Gestion des risques transactionnels

Cas concret: MultiLine

ATEL: mai 2008

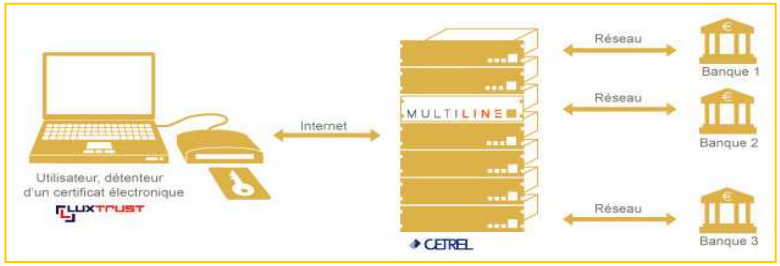
Roll-out depuis février 2008

Les services offerts:

- virements et domiciliations en saisie manuelle online et upload
- extraits en consultation online et download + intraday

Les nouveautés (rappel):

- authentification et signature électronique LuxTrust
- webbased (ADSL)
- un seul point d'accès (login et helpdesk technique)
- userfriendly



Les futures évolutions 2008/2009:

- hash commercial : résultat d'un calcul sur un fichier qui garantit sa non-altération lors de son transfert vers ML
- Isagate Corporate: application de transfert automatique pour uploader + recevoir des fichiers entre le système interne du client et ML (cible: grandes entreprises) / application installée directement chez le client
- améliorations diverses

Principaux risques encourus par une entreprise recourant à une application transactionnelle …

Risque qu'une personne non-habilitée

- accède à l'application
- réalise des transactions de virement ou de consultation moyennant l'application
- accède à un compte sur lequel elle ne dispose pas d'un droit de pouvoir

Risque qu'une personne

- dépasse ses pouvoirs de disposition sur un compte
- conteste avoir réalisé la transaction

Risque de

- perte des instructions lors de la transmission
- contestation sur la date, l'heure de dépôt de l'instruction / de la livraison à la banque (contexte respect de cut-offs)
- ne pas pouvoir reconstruire l'historique d'une transaction

Conséquences des risques déterminés pour l'entreprise

Le risque	Impact éventuel pour l'entreprise
Accès non-autorisé	Risque de pertes financières pour l'entreprise et éventuellement d'image de marque
Transaction non-autorisée	
Accès à un compte non-autorisé	
Pouvoirs de signature dépassés	
Transaction contestée	
Perte de données	
Dépassement des cut-offs	
Pertes de traces	

En vue de se protéger au maximum contre ces risques et les conséquences y relatives, l'entreprise attend que l'application transactionnelle qu'elle utilise lui fournisse les moyens nécessaires

Les banques ont investi beaucoup dans la sécurisation du New-ML

Affronter ces risques …
à travers l'exemple ML (1)

Le risque	Moyen mis en œuvre par les banques pour contrecarrer le risque
Accès non-autorisé	Tous les utilisateurs d'une entreprise ont besoin d'un certificat LuxTrust afin de s'authentifier auprès de l'application. Une personne non-habilitée ne peut ainsi pas accéder au système. NOK de l'authentification → refus de l'accès à l'application
Transaction non-autorisée	Les pouvoirs individuels des utilisateurs sont définis dans la convention MultiLine à signer avec chaque banque. La banque reprend ces pouvoirs dans l'application. Un utilisateur peut seulement faire les transactions qui lui sont autorisées (ex: uniquement saisie, mais pas validation).
Accès non-autorisé à un compte	Les accès individuels aux comptes par les utilisateurs sont définis dans la convention MultiLine à signer avec chaque banque. La banque reprend ensuite ces accès dans l'application. Un utilisateur ne peut consulter et accéder que les comptes qui lui sont autorisés!
Pouvoirs de signature dépassés	Les pouvoirs de signature (*qui* peut signer pour *quel* montant de transaction sur *quel* compte) sont définis dans la convention MultiLine avec chaque banque et ensuite repris par la banque dans l'application MultiLine. L'application contrôle lors de chaque transaction à signer les pouvoirs de signature.

Affronter ces risques …
à travers l'exemple ML (2)

Le risque	Moyen mis en œuvre par les banques pour contrecarrer le risque
Transaction contestée	Le client/l'entreprise est responsable de la bonne utilisation du certificat LuxTrust par ces utilisateurs. Toutes opérations/instructions ordonnées conformément à la convention sont opposables au client/à l'entreprise et sont censées émaner de lui/d'elle. L'utilisation correcte des moyens d'authentification constitue la preuve irréfutable, complète et valable de l'identité de l'utilisateur et en cas de signature électronique apposée par l'utilisateur.
Perte de données	- L'authenticité, l'intégralité et la confidentialité des ordres sont assurées par l'utilisation de la sécurité LuxTrust. La gestion du flux des informations est assurée par un système d'accusés de réception techniques à tous les niveaux. - Dédoublement de l'infrastructure technique pour éviter les pertes de données en cas d'incident technique. - Backups pendant la journée pour éviter la perte de données en cas de problème de software. - HASH commercial: mécanisme permettant de vérifier l'exactitude de ce qui a été envoyé (future évolution!)

Affronter ces risques …
à travers l'exemple ML (3)

Le risque	Moyen mis en œuvre par les banques pour contrecarrer le risque
Dépassements cut-offs	La banque et le client acceptent que l'enregistrement informatique effectué par la banque, quel que soit son support, constitue une preuve probante et suffisante de l'identité de l'utilisateur, du contenu et des modalités d'exécution des ordres donnés par l'utilisateur (convention MultiLine).
Perte des traces	Toutes les transactions sont loggées et conservées/archivées pendant une durée de 10 ans.

LuxTrust a été développé en vue de répondre au mieux aux besoins de ses clients tant au niveau de la sécurité qu´au niveau de l´utilisation quotidienne de l'Internet.

Produits de LuxTrust

- Smartcard
- Signing server token / SMS
- Signing stick
- Certificats SSL et certificats objet
- Trusted time-stamping
- Solutions PKI sur mesure

Applications B2B supportant déjà la sécurité de LuxTrust

MultiLine e-TVA
PLDA (Paperless Douanes et Accises)
Registre de Commerce et des Sociétés
Sofie Bourse de Luxembourg
Portail Santé

Futures évolutions de LuxTrust dans 'B2B'…

Application e-Gouvernement à destination des personnes privées

Pour de plus amples détails: prière de consulter www.luxtrust.lu

LUXTRUST

Important …
malgré les préventions et les mesures
mises en place par les banques MultiLine ….

Le client/l'entreprise doit veiller

. à la bonne gestion des droits d'accès de son personnel à l'application ML et aux droits de disposition sur ses comptes

. e.a. à ce que son infrastructure Internet soit sécurisée (antivirus, firewall)

. à la bonne conservation et gestion de ses certificats LuxTrust et des mots de passe y relatifs ainsi qu'au renouvellement de ces derniers.

IFCC

Institut de Formation de la Chambre de Commerce

a·t·e·l

Association des Trésoriers d'Entreprise à Luxembourg

MULTILINE

BANQUE ET CAISSE D'EPARGNE DE L'ETAT LUXEMBOURG

DEXIA

BGL BNP PARIBAS

Banque Raiffeisen

SOCIETE GENERALE

ING

BANQUE DE LUXEMBOURG

P&T LUXEMBOURG