LA PROTECTION ET LA SECURITE DES TRANSACTIONS DANS UNE RESEAU INFORMATIQUE INTERBANCAIRE

Mihalcescu Cezar

Universitatea Româno Americană, Calea 13 Septembrie 104, Bl 48, Ap 21, sector 5, Cod Postal 050727 Bucureşti, Tel 0722-387-162, e-mail cezar_mihalcescu@hotmail.com

Ciolacu Beatrice

Universitatea Româno Americană, e-mail : beatrice_ciolacu@yahoo.com

Pavel Florentina

Universitatea Româno Americană, e-mail: pav_florentina@yahoo.com

Titrade Cristina

Universitatea Româno Americană, e-mail: cristina_titrade@yahoo.com

Les transactions électroniques deviennent de plus en plus complexes, grâce au système qui se développe de manière permanente, aux technologies d'équipements et aux logiciels, ainsi qu'à l'environnement virtuel dans lequel ils opèrent (Internet ou Réseaux à Valeur Ajoutée). La valeur de l'information s'appuie sur son intégrité et, dans le cas où le système de sécurité ne permet pas la réalisation de cette demande, l'information va perdre sa signification.

Les institutions financières utilisent des jetons d'authentification générateurs de mots de passe pour identifier les clients commerciaux afin de permettre l'accès à distance au système des opérations via Internet. L'infrastructure de clé publique (PKI) peut incorporer des cartes à puces intelligentes qui contiennent l'accréditation de l'utilisateur et un certificat numérique

Keywords : sécurité électronique, l'information, e-banking

La sécurité électronique est définie par certains experts comme « les politiques, recommandations et actions nécessaires afin de minimiser le risque afférent aux transactions électroniques, risque qui se réfère en particulier aux créneaux dans le système, des intrusions ou vol ». autres la définissent comme « tout moyen, technique ou processus utilisé pour protéger le volume d'information d'un système ». La valeur de l'information s'appuie sur son intégrité et, dans le cas où le système de sécurité ne permet pas la réalisation de cette demande, l'information va perdre sa signification. Dans ce contexte, les spécialistes de la Banque Mondiale considèrent que la sécurité représente une modalité de créer de la plus valeur, devenant ainsi une préoccupation majeure de l'institution pour laquelle doit s'implémenter.

Ainsi, la Banque Mondiale recommande un système de sécurité des opérations bancaires déroulées via Internet, qui soit structuré sur 12 niveaux : le responsable avec la sécurité, l'authentification, firewalls, le filtrage active du contenu, le système de détectage des intrusions, les logiciels antivirus, le cryptage, le teste de la vulnérabilité, l'administration adéquate du système, les applications de gestion de la politique bancaire et le plan d'action contre les incidents. Les aspects-clé du fonctionnement d'un système de sécurité sont : l'accès, l'authentification, la confiance, la non- rejection, la confidentialité et la disponibilité.Les banques prendront des mesures adéquates pour vérifier et authentifier le niveau de l'autorisation des clients qui font des opérations d'e-banking sur leur propre réseau bancaire. L'authentification comprend deux processus : l'établissement de l'identité des nouveaux clients et l'autorisation des nouveaux clients ou de ceux qui existent déjà. La vérification de l'identité fait référence aux procédures, aux techniques et aux processus employés pour établir l'identité d'un client lorsque celui-ci ouvre un compte. L'autorisation fait références aux procédures, techniques et processus utilisés pour déterminer si un client ou un employé a le droit d'accès à un compte bancaire ou l'autorisation d'effectuer une certaine transaction sur ce compte bancaire.

Dans toute opération, il est essentiel de confirmer si un certain canal de communication, une transaction ou une demande d'accès est légitime dans le contexte de sécurité donné. Dans ce sens, les banques développeront des mesures de vérification de l'identité et d'autorisation des nouveaux clients, de la même manière et avec les mêmes procédures que pour les clients existants au moment de l'initiation des

transactions électroniques. La vérification des clients pendant la déclaration du compte d'utilisateur est très importante, réduisant les risques de validation d'identités frauduleuses d'accès aux applications de scannage et de vol des comptes d'accès. Les erreurs d'une banque dans l'authentification des clients peuvent avoir des effets très graves, des fraudes contre la banque, de l'atteinte à l'image de celle-ci, des écoulements d'informations confidentielles et jusqu'à l'implication de la banque dans d'autres opérations de fraude d'autres entreprises ou à la transgression des normes financières locales.

Les banques utiliseront des méthodes d'authentification des transactions pour ne pas rejeter et pour enregistrer les opérations sur les comptes des clients via e-banking. Le fait de ne pas rejeter les opérations garantit l'intégrité de l'origine des transactions du point de vue de l'expéditeur. De cette façon, l'expéditeur de la transaction électronique est empêché de rejeter la réalisation de la transaction. Il est possible également de vérifier si la transaction n'a pas été altérée à une date ultérieure. A cause du risque assez élevé dû aux difficultés d'identification et d'autorisation des entités en cours de négociation, il est possible que les transactions ayant subi des altérations ou des détournements puissent être l'objet de réclamations des clients afin de les rejeter.

Pour réduire ces effets, les banques doivent faire des efforts considérables afin de s'assurer que :

- Les systèmes e-banking ont été prévus afin de réduire le nombre de transactions mal transmises, et les utilisateurs comprennent les risques associés à toute transaction qu'ils réalisent ;
- Toutes les entités impliquées dans une transaction sont clairement identifiées et autorisées, et la communication se fait sur un canal sécurisé. Le système e-banking devra garder le contrôle de la sécurité du canal de transmission en cours de transaction ;
- Les transactions financières sont protégées contre les possibles altérations qui, si elles surviennent, doivent être détectées.

La modalité pratique pour réaliser tout cela est d'utiliser les certificats numériques par une infrastructure de clés publiques ou de signature électronique, technique reconnue légalement dans plusieurs pays du monde.

Les Étapes dans l'établissement des politiques de sécurité

• **Établir les objectifs de sécurité**. En planifiant les conditions requises pour la sécurité d'un système, il faut tenir compte d'une série d'objectifs :

- confidentialité – il s'agit de protéger l'information contre une lecture ou un copiage par des utilisateurs qui ne sont pas explicitement autorisés à ce faire ;
- intégrité des données – protège les données contre les altérations ou les pertes accidentelles ou voulues ;
- disponibilité – impossibilité de désactiver un service sans droits octroyés en ce sens ;
- contrôle – définit l'accès au système, en protégeant le système contre l'accès non autorisé des utilisateurs ou des programmes ;
- audit – permet l'identification des problèmes apparus et met en relief les dommages subis. pour cela il faut qu'il existe des enregistrements (journaux) des activités du système. Cet objectif en milieu bancaire est plus important que la confidentialité ou la disponibilité.

• **Définir les risques**. Cette étape impose l'analyse de tous les risques existants, après quoi peuvent être panifiées des politiques et techniques adéquates de protection.

L'analyse des risques peut se faire par l'intermédiaire de plusieurs méthodes, l'une tournée vers le volume des risques, les autres vers le volume des coûts :

- **MARION** – est une méthode utilisée dans le milieu bancaire et des affaires, développée en plusieurs sous ensembles, comme suit :

MARION-AP	pour l'analyse des risques pour les ordinateurs séparés	IBM PC/APPLE
MARION – RSX	pour l'analyse au niveau des grands réseaux	main frame
MARION – PMS	pour l'analyse des petites affaires	IBM PC/APPLE

MARION – H	pour la gestion des ressources humaines	main frame

- **CRAMM** – méthode se préoccupant des risques et non les coûts ;
- **NIST** (National Institute of Standards and Technology) et NCSC (National Computer Security Center), apparues aux États-unis, ont mis au point un ensemble d'applications pour le développement de la recherche dans le domaine des méthodologies et des techniques de maîtrise du risque.

• **Calculer la faisabilité.** Est composé de deux éléments :

a) le coût de production, qui doit tenir compte des coûts des réparations/remplacements, des arrêts de travail, de l'image de la société bancaire, etc. En général, ces coûts sont estimés sur une échelle de coût minimal et maximal ;

b) le coût de la prévention, qui doit évaluer, en argent, les coûts imposés par les techniques destinées à contrecarrer chaque menace. Évidemment, plus la solution de sécurité est complexe, plus son coût est élevé.

• **Réaliser les politiques de sécurité, en concordance avec les objectifs**. Au cours de cette étape, est définie une politique générale de règles destinées à l'ensemble des services ou sous-domaines, suivie de politiques particulières pour divers biens protégés.

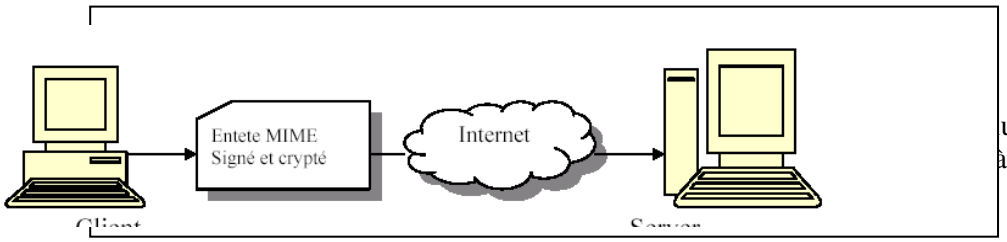
• **L'audit et la qualité des mises en application**. C'est une étape très importante, vu qu'au cours de cette étape il peut être constaté si la politique de sécurité fonctionne et sur quels paramètres. C'est une activité continue ayant le rôle de réglage de la politique de sécurité.

La sécurité dans les systèmes d'Internet Banking

Les créateurs de la version initial du protocole HTTP se sont proposés de créer une méthode de communication des informations multimédia (graphique, vidéo, audio). mais ils se sont vite rendu compte que HTTP deviendra la colonne vertébrale d'un incroyable nombre d'applications commerciales. Au fur et à mesure que le Web ait commencé a être utilisé de plus en plus pour des raisons commerciales, tant les entreprises que les utilisateurs particuliers ont reconnu la nécessité de la sécurité des transactions de type « end-to-end », en défit des transactions pas assurés de type « hop-by-hop ». Afin de répondre aux demandes de plus en plus accentuées pour des standards de sécurité sur le Web, Internet Engineering Task Force a lancé une demande de proposition en 1994. S-HTTP a été conçu par Entreprise Integration Technologies (EIT) comme résultat de cette demande.

S-HTTP (Secure Hypertext Transport Protocol) est une version modifiée de HTTP (Hypertext Transport Protocol) qui inclue des facilités supplémentaires de sécurité.

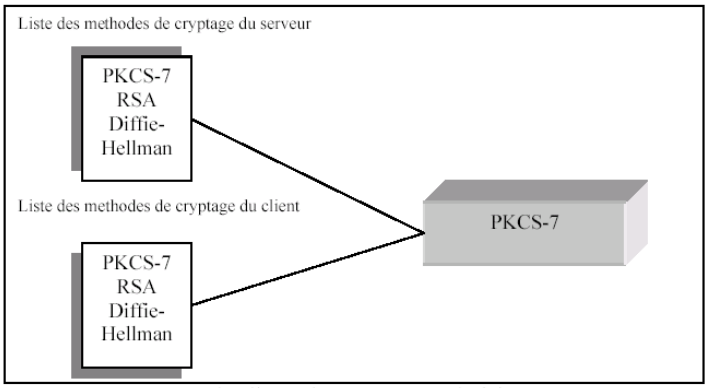
Les implémentations S-HTTP comprennent le cryptage des documents Web envoyés par Internet, et le support pour les signatures digitales. S-HTTP permet au client (browser) la capacité de vérifier l'intégrité des messages Web en utilisant un code d'authentification des messages (Message Authentification Code – MAC). S-HTTP éteint le modèle de transaction HTTP et les caractéristiques d'une transaction pour implémenter en HTTP le support de sécurité. La conception S-HTTP offre des communications sures entre un client et un serveur HTTP. Le but principal de S-HTTP set celui de permettre des transactions commerciales entre différentes types d'applications. Les différentes méthodes utilisées par S-HTTP pour assurer la sécurité du message comprennent une méthode de signature, une méthode de cryptage, un utilitaire de transmission des messages et des vérifications de la signature.



ajoute
us de
à HTTP

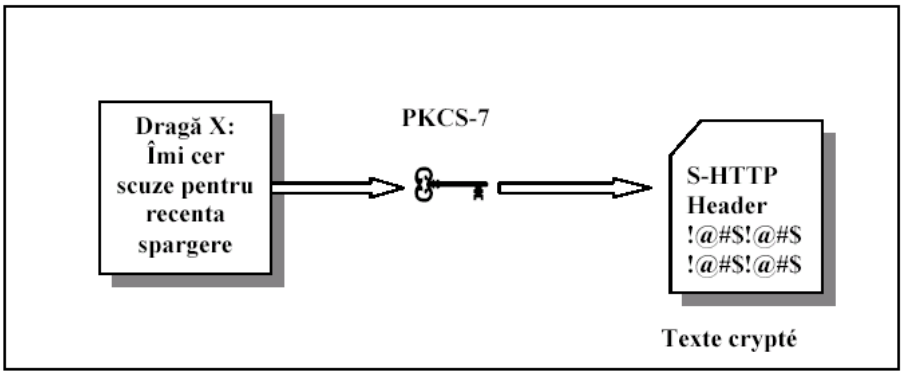
Les messages HTTP contiennent deux éléments principaux : l'entête du message (indique au destinataire la modalité du traitement) et le corps du message (par exemple, un entête qui indique le fait que le MIME du corps du message est de type Text/HTML demande au récepteur de traiter le corps du message comme un doc HTML (Hypertext Markup Language).

Afin de créer un message HTML< le serveur combine ses propres préférences de sécurité avec celles du client. Par exemple, si le serveur est défini comme Public key Encryption Standard 7 (PKCS-7) et la liste de cryptage du client comprend PKCS-7, le serveur va crypter le message utilisant PKCS-7, comme suite :

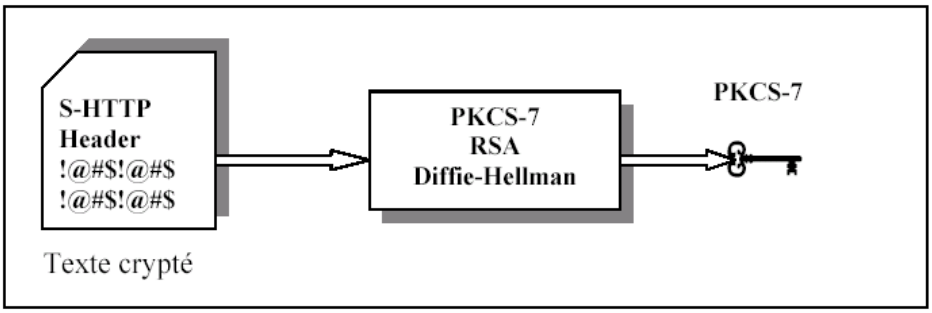


Le serveur compare les listes de cryptage et choisi PKCS-7

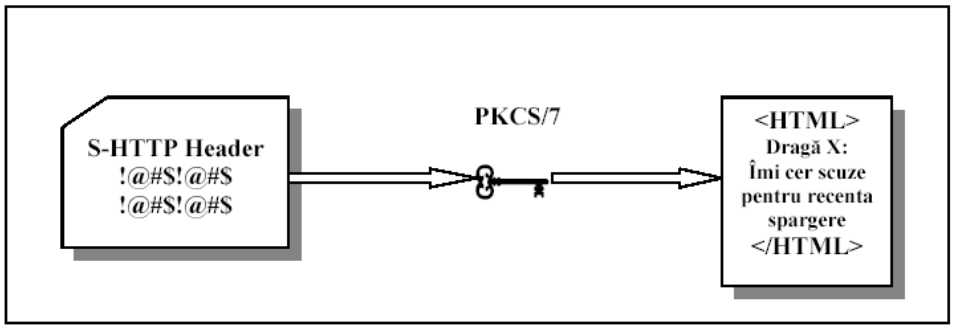
En appliquant une méthode de cryptage acceptée tant par le client que par le serveur, le serveur va crypter le message de type simple texte afin de créer le message S-HTTP. n continuation on représente la modalité de cryptage d'un message par le serveur et la création du message cripté.



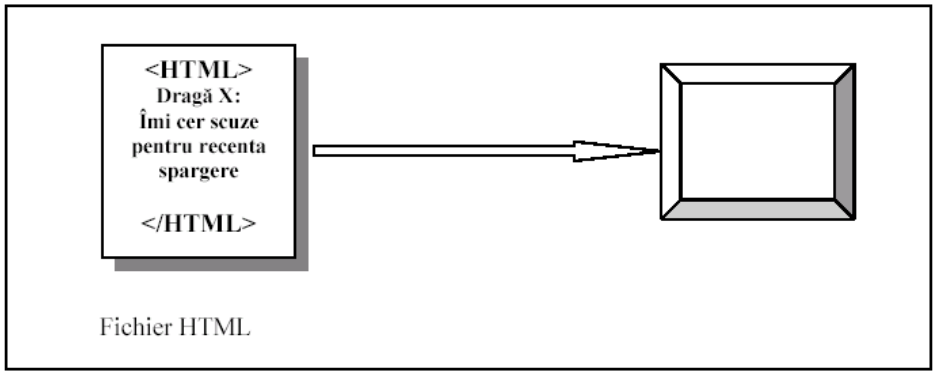
S-HTTP utilise trois données d'entrée pour créer un message HTTP : la transmission du texte simple, les préférences de cryptage du client et celles du serveur. A son tour, le destinataire du message (le client) utilise trois données d'entrée similaire afin de décrypter le message S-HTTP et pour accéder au texte du message. Pour décrypter le message S-HTTP, le client doit lire l'entête pour découvrir les transformations cryptographiques apportées par le serveur au message :



Apres avoir identifié le standard du cryptage indiqué dans l'entête du message par comparaison avec un des systèmes de cryptages connus, le client décrypte le message utilisant une certaine combinaison entre le matériel des clés de l'émetteur et celui du récepteur. Dans la suivante schéma, le client appliquera au message S-HTTP sa propre clé privée pour décrypter le message :

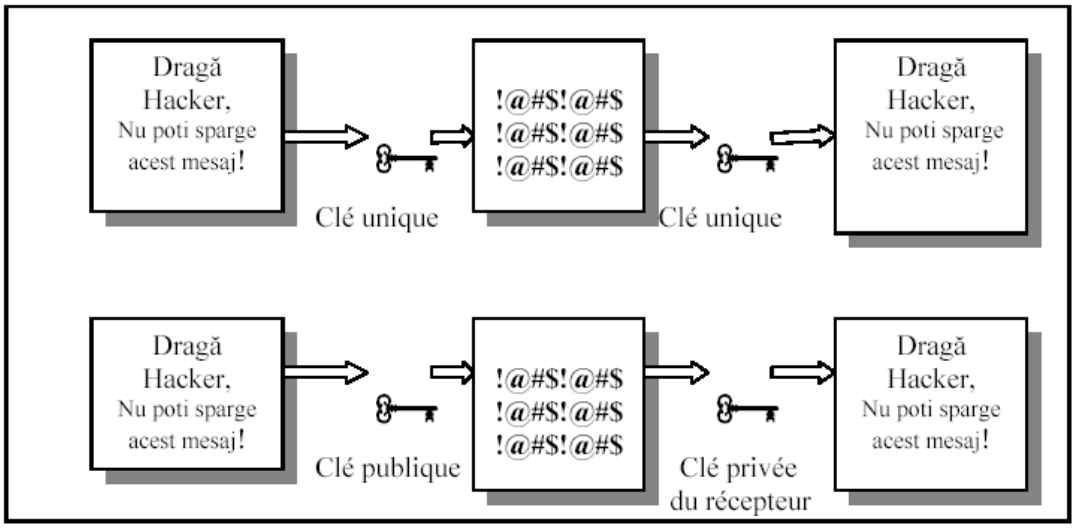


Après avoir décrypté le message, le client va lister les données HTTP encapsulées ou les autres données dans son browser :

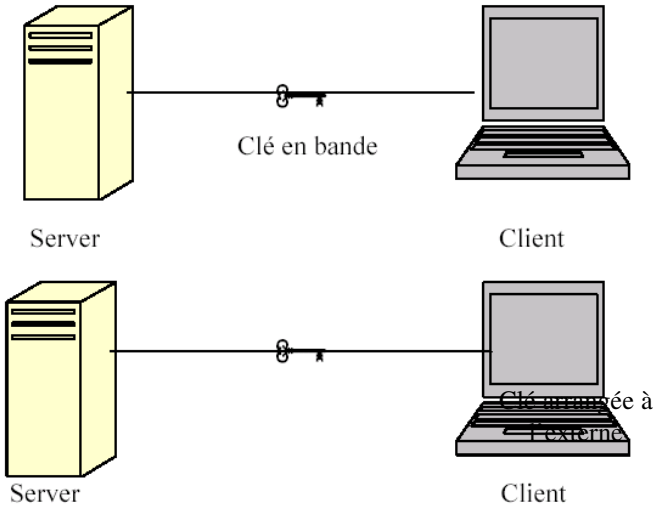


Dans un crypto système avec clé symétrique, les 2 parties utilisent la même clé pour crypter/décrypter les messages. En utilisant S-HTTP, les seuls qui connaissent la clé sont le client et le serveur, fait qui contribue à assurer la confidentialité. Le crypto système avec clé asymétrique dispose de 2 clés distinctes : une clé publique (à disposition de tout le monde) et une clé privée, qui diffère selon l'utilisateur. Pour transmettre un message confidentiel en utilisant un crypto système avec clé asymétrique, l'émetteur utilise la clé publique du récepteur pour crypter le message. Le crypto système avec clé asymétrique assure une totale confidentialité puisque uniquement le récepteur dispose de la clé privée nécessaire (propre) avec laquelle on peut décrypter le message.

Les crypto systèmes avec clé symétrique et asymétrique :

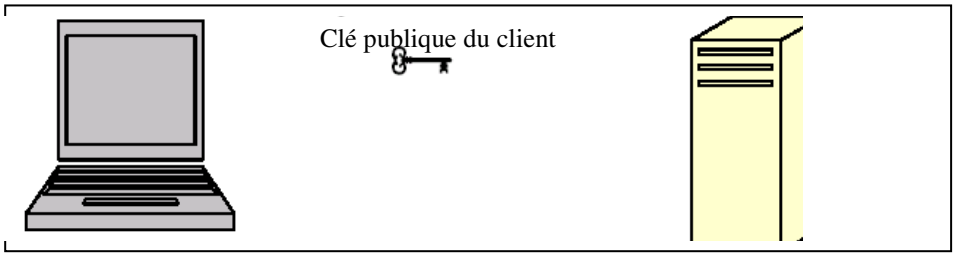


S-HTTP a défini deux mécanismes différentes de transfert/utilisation des clés. Le premier transfère la clé publique « en bande » et l'autre utilise des clé arrangées à l'externe. Dans le premier cas, le serveur crypte la clé privée en utilisant la clé publique du client et la renvoi à celui-ci. Dans la deuxième méthode, utilisée plus largement dans les systèmes Intranet des entreprises, le client et le serveur réalisent le transfert des clés manuellement. Etant donné que la plupart des utilisateurs ont accès aux clés via le WEB, la première méthode est utilisée dans la grande majorité des cas.

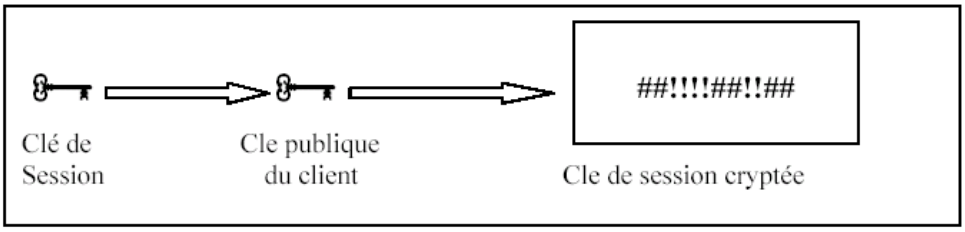


Pour mieux comprendre le transfère « en bande », voyons la modalité dans laquelle le client et le serveur interfèrent au moment où le client visite un site Web sure. La transaction HTTP se réalise dans les suivantes étapes :

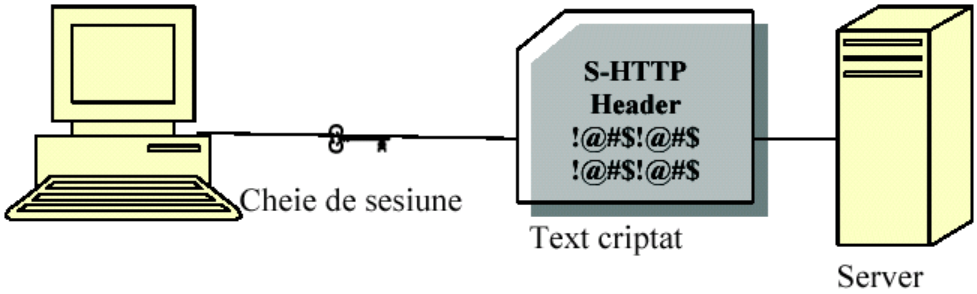
- quand le client visite le site Web S-HTTP, il envoi une demande de connexion vers le serveur pour initier la transaction. A son tour, le serveur va toujours répondre avec un message « Connexion réussite » (Connection Successful).
- Après avoir reçu ce message, le browser du client va transmettre au serveur sa clé publique et le crypto système dans le cadre duquel le client s'était fait créer sa clé publique (RSA, PKCS-& etc) :



– Après réception de la clé publique du client, le serveur consulte la liste des crypto systèmes acceptées, pour vérifier s'il peut accéder ainsi à la clé publique du transfert :



Après avoir établi une connexion réussite avec le serveur, le browser du client crypte chaque transmission adressée au serveur en vertu de la clé de session :



Appart S-HTTP, les serveurs utilisent d'habitude aussi un deuxième protocole, Secure Soket Layer (SSL) – pour assurer une communication sécurisée avec les clients.

A mentionner aussi que S-HTTP accepte une large variété de mécanismes de sécurité pour les clients et les serveurs HTTP.

Conclusion

Établir clairement les spécifications du système e-banking dans le but d'organiser des flux de données et des procédures de travail pour chaque système bancaire (bases de données ou applications). La division des attributions entre les sous systèmes est une mesure de contrôle interne, prévue pour réduire le risque de fraude dans les processus opérationnels, assurant l'autorisation correcte, l'enregistrement et la conservation en sécurité des transactions électroniques. Cette méthode est importante afin d'assurer l'exactitude et l'intégrité des données, mais aussi en tant que méthode de prévention de la propagation des transactions frauduleuses à tous les niveaux du système. Si les attributions des sous systèmes sont bien déterminées, une possible fraude produira des dommages uniquement lors de la tentative de pénétration dans le système, sans affecter les autres niveaux.

Vu l'ingéniosité des personnes ou des organisations malveillantes pour dissimuler de fausses transactions, cette méthode de sécurité doit également faire l'objet d'entretien et d'adaptations continuelles.

Bibliografie

1. Basno C., Dardac N., *Management Bancar*, Editura Economică,
2. Bucureşti, 2002
3. Butler C., *Mastering Value at Risk*, Editura Financial Times Pitman
4. Publishing, Londra, 1999
5. Chapman C., Ward S., Project risk management. Processes, Techniques
6. *and Insights*; Editura Wiley & Sons, Anglia, 1997
7. Collinge A., Strategic Management of E-Commerce Risk in IT Directors
8. Strategy Meeting 2002 – Executive perspectives, 2002
9. Coult H. V., *Management in banking,* Editura Pitman Publishing, Londra,