Proposition de solution : chèque numérique

Louis BILLIET
Florent DAVID

25 Sept. 2013

1 Sujet

Le but de l'exercice est d'imaginer un système de chèque numérique permettant à un client de payer un vendeur. Le chèque represente un ordre de virement de compte client au compte vendeur que la banque doit effectuer.

La connexion avec la banque est payante. Pour limiter les frais, nos vendeurs souhaitent grouper les chèques. La connexion avec la banque est non garantie (donc différé en cas d'echec).

Il existe divers canaux de communication : entre vendeur et banque et entre client et vendeur.

L'outil d'émission de chèque est fournit par banque au client (pas via le vendeur).

But de l'exercice : Concevoir les 3 logiciels de manière securisé : génération de chèque, vérification du chèque et encaissement du chèque.

Attention :
- Le client peut être un bandit !
- Le vendeur peut être un bandit !
- La banque ne peut être qu'une banque ! Merci la banque !

2 Conventions de nommage

Soient :
- A.Kpub la clé publique d'Alexandre.
- B.Kpriv la clé privée de Benjamin.
- C.rib la relevé d'identité banquaire de Charlie.
- D.facture une facture emise pas Dominique.
- E.paiement l'ordre de paiement venant d'Edouard.
- C(F.rib, G.Kpriv) le rib de Frederic chiffré avec la clé privée de Geraldine.
- H.HRid l'identifiant "Human Readable" de Henri.

Nous parlerons dans cet exercice de Victor, le vendeur, de Charles, le client, de Boris, le bandit et de Banque, la banque (nous ne ferons pas de publicité ici).

3 Analyse et présuppositions

Étant donné que le client et le vendeur payent ici avec un compte en banque, nous supposons qu'ils y ont au préalable ouvert un compte. Nous supposons ici que :
- Victor, Charles, Boris et Banque ont déjà généré leurs paires de clé publique/privée.
- Banque fournis à chaque personne ouvrant un compte (qu'on apellera Pierre) un certain nombre d'informations, dont C(P.HRid+P.RIB+P.Kpub, Bq.Kpriv).

Nous supposons de plus que Banque connais les informations suivantes :
- Bq.Kpub
- Bq.Kpriv
- V.RIB

- V.Kpub
- V.HRid
- C.RIB
- C.Kpub
- C.HRid

Nous supposons de plus que Victor (ainsi que Charles et Boris) connaissent les informations suivantes :

- Bq.Kpub
- V.Kpub
- V.Kpriv
- V.RIB
- V.HRid
- C(V.HRid+V.rib+V.Kpub, Bq.Kpriv)

4 Proposition de solution

4.1 format des communications

Dans un premier temps, lorsque Victor annonce le montant à Charles, il lui transmet 5 informations :

- V.HRid
- V.rib
- le montant
- un numéro de transaction unique pour le vendeur
- le "certificat" de la banque

Le message de Victor vers Charles aura donc la forme :

C(montant+transactionID, V.Kpriv)+C(V.HRid+V.RIB+V.Kpub, bq.Kpriv)

Pour payer Victor, Charles doit lui transmettre :

- V.rib
- le montant
- le numéro de transaction
- C(C.HRid+C.rib+c.Kpub, Bq.Kpriv)

Donc, le chèque aura la forme :

C(V.RIB+montant+transactionID, C.Kpriv)+C(C.HRid+C.RIB+C.Kpub, bq.Kpriv)

4.2 Tests réalisés

Lorsque Charles reçoit une demande de paiement, il déchiffre

C(V.HRid+V.RIB+V.Kpub, Bq.Kpriv)

avec Bq.Kpub afin de récupérer V.HRid. Il vérifie que V.HRid est bien celui de Victor (test humain). S'il pense que c'est bon, il émet un chèque à Victor avec les autres données extraites.

Lorsque Victor reçoit un chèque, il déchiffre

C(C.HRid+C.RIB+C.Kpub, Bq.Kpriv)

avec Bq.Kpub afin de récupérer C.RIB et C.Kpub. Il utilise Kpub pour déchiffrer

C(V.RIB+montant+transactionID, C.Kpriv)

puis compare V.RIB, montant et transactionID avec celui qu'il a émit à Charles. Si les informations sont cohérentes, la chèque est valide.

Lorsque la banque reçoit un chèque, il déchiffre

C(C.RHid+C.RIB+C.Kpub, Bq.Kpriv)

avec Bq.Kpub afin de récupérer C.RIB et C.Kpub. Il utilise Kpub pour déchiffrer

C(V.RIB+montant+transactionID, C.Kpriv)

puis vérifie si le couple (V.RIB, transactionID) n'a pas déjà été utilisé dans un autre chèque. S'il n'y a pas de problèmes, il peut débiter *montant* du compte C.RIB et créditer cette somme sur le compte V.RIB.

5 Scenarii d'attaque parées

5.1 Boris veut intercepter le chèque de Charles

Borris ne peut pas remplacer C(V.RIB+montant+transactionID, C.Kpriv) pour créditer son propre compte, étant donné qu'il ne connais pas C.Kpriv. La banque refusera le chèque, car la partie remplacée n'a pas été

chiffré avec C.Kpriv mais avec B.Kpriv.

5.2 Boris intercepte la facture de Victor et y remplace le RIB par le sien

Si Boris veut intercepter la facture émise par Victor et y mettre son RIB à la place de celui de Victor, il devra forger une toute nouvelle facture. Si Charles ne veut pas se faire avoir, il devra vérifier qui est l'émeteur de la facture.

5.3 Boris veut payer Victor avec le "chèquier" de Charles

Victor recevra un message qui ressemblera a
C(V.RIB+montant+transactionID, B.Kpriv)+C(C.HRid+C.RIB+C.Kpub, bq.Kpriv).
Victor ne sauras pas déchiffrer C(V.RIB+montant+transactionID, B.Kpriv), étant donné qu'il n'a pas été chiffré avec C.Kpriv mais avec B.Kpriv.

5.4 Victor veur encaisser plusieurs fois le chèque de Charles

Lorsque Victor émet une facture, cette facture contient un numéro de transaction. Lorsque Charles émet un chèque, ce chèque contient ce même numéro de transaction. Si Victor essaie d'encaisser plusieurs fois le même chèque, Banque verra passer plusieurs fois le même numéro de transaction pour le même RIB. La banque rejetera donc les ré-encaissements d'un même chèque.

5.5 Victor veut augmenter le montant du chèque

Lors de la création du chèque, Charles chiffre les informations concernant le destinataire (et notemment le montant) avec sa clé privée. Sachant que la clé publique correspondante est chiffrée par la banque dans le certificat, si Victor veut altérer le montant, il faudra qu'il re-chiffre cette partie du chèque avec la clé privée correspondante (celle de Charles). Information que seul Charles détiens (en principe).

5.6 Charles veut réutilser un chèque déjà utilisé

Lors de l'émission de la facture, Victor génère un numéro de transaction unique. Si Charles veut utiliser un chèque déjà utilisé, il devra fatalement y apposer un numéro de transaction qui a servi pour une autre facture. Or, si le numéro de transaction du chèque ne correspond pas avec celui de la facture, le paiement sera rejeté directement par Victor.

5.7 Charles paye pour une facture qui ne le concerne pas

Hélas, dans ce cas, Charles aurait dû vérifier ce pour quoi il paie.