Public Electronic Contract Protocol

Tak-Ming Law

Hong Kong Institute of Vocational Education (Morrison Hill)
Department of Computing, 6 Oi Kwan Road, Wan Chai, Hong Kong.
Email: tmlaw@vtc.edu.hk

Abstract. The notion of Public Electronic Contract (PEC) Protocol is presented in this poster paper. In the idea, the PEC will be published on a public directory (of certain groups) and let all the members to review the true (raw) transaction information. Collection of information of PEC reflects more reliable facts of the market trends rather than merely depends on the data provided by certain agencies for estimation. The goal is to eliminate the opportunities for certain agencies to manipulate the data and persuade the investors to make inappropriate decisions on purchases or investments. A perfect open market with open facts should be established in the future. The PEC also contains the property of public witnesses so that the transactions will be more secure. In order to keep the protocol simple; its implementation is mainly based on RSA public key scheme.

Key words: publics, contracts, transactions and signatures.

1 Introduction

Is it beneficial for a party, the customers and vendors who complete their transactions by electronic forms, agree to disclose all of their information of purchase on a public directory so that the market becomes *absolutely* public? To me, the answer is *yes*. I have the following assumptions.

Assumption 1: *The information of transaction in the free market is still translucent (not totally open).*

I call the market is *translucent* when its revealed data are *not* absolutely accurate and *not* totally open to the public. Usually, the customers and vendors will not disclose their contracts of transaction in the public. The customers only can estimate the trends of the market prices based on the information provided by the vendors. Nonetheless, how can the customers know the information is reflecting the real facts of actual situations in the markets or just *make-ups* from the vendors? Therefore, the one-sided stories prepared by the vendors are possibly processed by "black-box" manipulations. In the stock and real estate markets, for example, the party usually will not publish their contracts after their deals and the actual information is only kept by the brokers and finally directed to the government agency. The *publics* (from now on, I call the potential customers or vendors who are looking for opportunities of purchasing or

selling goods and services as ***publics***) have no means to obtain the original information unless the government agency or brokers reveal the data at the time they prefer. In some situations, the customers or investors are confused by bias statistics provided by certain agencies. As noted before, the publics in no ways to acquire the *raw* data immediately after the transactions and prove its correctness. Is it fair to the publics?

Assumption 2: *There are no public channels for the publics to collect or analysis* ***individual*** *and* ***original*** *facts.*

The *publics* have ways to survey through reports and publications for the market prices trends. Nevertheless, they are certainly not able to review the contents of individual transaction. In other words, the publics merely depends on the information and analysis provided by other parties to make their decisions of purchase. From the investment points of view, it is a very dangerous decision making procedure.

Due to the above two assumptions, I am motivated to design a protocol that will be capable to reveal and maintain the true facts of the previous transactions in the market. As the E-commerce grows rapidly, I assume the future transactions are mainly traded on the Internets. Consequently, the protocol is named as *Public Electronic Contract* and abbreviated as "PEC". The constructions of PEC are based on the RSA public key scheme [1]. Instead of keeping information in private, PEC tends to uncover the raw facts and primitives of transactions to the publics. I choose the concept of Contract to reflect the raw facts of transactions to the publics because it contains the fundamental information that both the customers and vendors agree, and which is enforced by laws. A definition can be concluded as follows.

Definition: *Public Electronic Contract (PEC) functions just like a regular contract we sign in the agents' or lawyers' offices. The only difference is its signing procedures are through electronic media. The commitments made in the contract are abided by the law and will be published on the public directory so that everyone can review its contents and be witness of the purchase.*

The notion of PEC is applicable to any kinds of transactions including goods and services. The contributions of PEC can be classified as follows.

Proposition 1: *Maintaining mutually fairness and confirmation between customers and vendors.*

As the contract is published on the public directory, all members (the *publics*) become witnesses of this transaction. The *boundedness* of the commitment between buying and selling becomes much rigid.

Proposition 2: *"Good" or "Bad" can be labeled on customers and vendors.*
Once the contract is signed, both selling and buying parties are under commitment. In case that a party fails to complete the transaction for whatever reasons, then the party's status is "bad" and which will also be published in the public directory. Therefore, the publics will know which customers or vendors are "good". Of course, the ones whose labels are "bad" will be panelized such as disqualifying them to do business on the net or put their names on the black lists to be reviewed by the publics.

Proposition 3: *The publics can analyze individual facts of transactions*
The publics become possible to reach and collect the individual facts, hence they can create applications to analysis the facts according to their own needs. Since the *publics* perform their unique analysis procedures, the results turn to be more independent, trustworthily and more valuable for individual necessity.

Proposition 4: *Mass witnesses of contract signatures*
As noted in proposition 1, the publics become witnesses of the contract. Whence, the contract will still be valid even though some of the witnesses are corrupted. Hence, the contract is protected publicly and simultaneously.

2. The Protocol

I introduce the protocol of PEC by a scenario. Suppose Alice and Bob are customer and vendor respectively. In the condition that they are both agree to disclose their transaction information in the public. The protocol consists of four steps as follows:

Step 1: Request for Purchase.
Step 2: Reply for confirmation of sales.
Step 3: Acknowledge of the receipt of goods.
Step 4: Acknowledge of the receipt of payment and the transaction completed.

2.1 Details

Step 1: Alice wants to purchase goods from Bob and sends him a Purchase Request which is encrypted by Alice's Private key.

1. A⇒B, Pub $\{P, T_0\}PRI\text{-}K_A$

P and $\mathbf{T_0}$ denotes Purchase Request order (PRO) and the time-stamp (time and date) of the order issued and signed. **P** consists of the name of purchasing item and proposed prices. The PRO is encrypted by Alice's private key $\mathbf{PRI\text{-}K_A}$ of RSA scheme so that the *publics* know that **P** and $\mathbf{T_0}$ are signed by Alice. The Purchase Request order $\{P, T_0\}PRI\text{-}K_A$ is published in a public directory **Pub** which might only be open to a certain groups of membership. From now on, the *publics* are able to verify the content and signature of the PRO by using Alice's public key.

Step 2: Bob decrypts the request by using Alice's public key. If Bob does not agree the proposed price for the item, he can negotiate with Alice by replying a message with a new proposed price on the same item requested by Alice. This negotiating process can be continued until both Alice and Bob agree on the price. The details of negotiation will not be published in **Pub**. Once both agree, Bob sends a Confirmation of Selling bounded with the previous PRO to Alice.

2. B⇒A, Pub $[\{P, T_0\}PRI\text{-}K_A, \{C,T_1\}PRI\text{-}K_B, CS(All\text{-}messages)]$

The current bounded message will replace the previous one in the public directory **Pub**. **C** and $\mathbf{T_1}$ denotes Confirmation of Selling and time-stamp (time and

date) of the confirmation issued and signed. **C** contains the confirmation statements that confirm Bob must sell the goods to Alice and the date of goods delivery (if necessary), and, again, which is encrypted with $\mathbf{T_1}$ by Bob's private key $\mathbf{PRI\text{-}K_B}$. **[]** in the protocol denotes the sense of bounding. **CS(All-messages)** denotes the cryptographic checksum of *All* the messages within the bound **[]**, using an algorithm such as the Secure Hash Algorithm (SHA) [2]. In this stage, the message published in **Pub** becomes the preliminary Public Electronic Contract (PEC) and the *publics* can verify and witness its contents and signatures as well. With the cryptographic checksum, **CS(All-messages)**, the publics will be able to detect discrepancies of the messages in the PEC. PEC is a *public-protected* Buy-and-Sell commitment, if either side fails to complete the transaction after this stage will subject to penalties.

Step 3: The transaction is not completed until the delivery-and-pay procedure has been settled. Once Alice received the goods from Bob and paid the bill, she should acknowledge immediately by bounding the acknowledgement with the PEC.

3. A⇒B, Pub [$\mathbf{\{R, T_2\}PRI\text{-}K_A}$, $\{P, T_0\}PRI\text{-}K_A$, $\{C,T_1\}PRI\text{-}K_B$, CS(All-messages)]

R and $\mathbf{T_2}$, encrypted by Alice private key $\mathbf{PRI\text{-}K_A}$, denotes the Receive of goods acknowledgement and time-stamp (time and date) of the acknowledgement issued and signed. The delivery company should ensure Alice acknowledge to Bob on the goods delivery. In this stage, the *publics* can verify it in the **Pub** as well (by Alice and Bob's public keys).

Step 4: After Bob receive Alice acknowledgment (decrypted by Alice's public key), he should acknowledge payment settlement to Alice and the publics as well.

4. B⇒A, Pub [$\{R, T_2\}PRI\text{-}K_A$, $\{P, T_0\}PRI\text{-}K_A$, $\{C,T_1\}PRI\text{-}K_B$, $\mathbf{\{E, T_3\}PRI\text{-}K_B}$, CS(All-messages)]

E and $\mathbf{T_3}$, encrypted by Bob's private key $\mathbf{PRI\text{-}K_B}$, denotes receipt of payment (completion of transaction) and time-stamp (time and date) of the acknowledgement issued and signed. This stage is the end of the transaction.

2.2 The PEC Protocol

The sequence of the PEC protocol is as follows:

1. A⇒B, Pub $\mathbf{\{P, T_0\}PRI\text{-}K_A}$
2. B⇒A, Pub [$\{P, T_0\}PRI\text{-}K_A$, $\mathbf{\{C,T_1\}PRI\text{-}K_B}$, **CS(All-messages)**]
3. A⇒B, Pub [$\mathbf{\{R, T_2\}PRI\text{-}K_A}$, $\{P, T_0\}PRI\text{-}K_A$, $\{C,T_1\}PRI\text{-}K_B$, **CS(All-messages)]**
4. B⇒A, Pub [$\{R, T_2\}PRI\text{-}K_A$, $\{P, T_0\}PRI\text{-}K_A$, $\{C,T_1\}PRI\text{-}K_B$, $\mathbf{\{E, T_3\}PRI\text{-}K_B}$, CS(All-messages)]

If the PEC published in **Pub** contains 4 messages, like
[$\{R, T_2\}PRI\text{-}K_A$,$\{P, T_0\}PRI\text{-}K_A$, $\{C,T_1\}PRI\text{-}K_B$, $\{E, T_3\}PRI\text{-}K_B$]
, it is shown that the transaction is completed. The PEC will stay in the **Pub** for a

period ***p***, say ***p***= publish-date + 15 days or publish-date + 30 days, etc. If current-date > ***p***, then PEC will be automatically deleted from the **Pub**. Here, publish-date denotes the date that the PEC published on the Pub and current-date denotes today's system date. In other words, the *publics* are permitted to review and witness the contents of PEC within the period ***p***.

One might feel that the above protocol is naïve. However, this protocol is still under development. More public key techniques, such as the Digital Signature Standard (**DSA**) [3], can be added into the protocol to make it more secure and sophisticated.

2.3 Private Remarks

Although the PEC is a public access contract, a right still preserved for both Alice and Bob to put *Private Remarks*, which the *publics* are unable to access, on the PEC. However, it is optional and not recommended. As mentioned in the beginning of this paper, everything should be treated publicly. An example for Private remarks is Alice's personal opinions about the services or goods from Bob or Bob's advises for Alice to complete the payment, etc.

If Alice wants to acknowledge private remarks that only Bob to know (or Bob's company staff), Alice can use Bob's public key $\mathbf{PUB\text{-}K_B}$ to encrypt it and bound it in the PEC. If Bob likes to acknowledge private remarks to Alice, just do it simultaneously as Alice.

3. Discussions and Conclusion

It is noticed that *Time Locks* [4] are also appropriate to be implemented in the PEC protocol. The goal of Time locks and time-release Cryptosystem is to reveal certain encrypted data *after* a predetermined time and no one can release the encrypted data, not even the one who encrypted it, *before* that time. In other words, both Alice and Bob are able to establish the publish-date and the period ***p*** upon agreement.

Alice and Bob have the right to decide the period of publication ***p*** by including the $\mathbf{TP_A}$ in the messages of step 1 and $\mathbf{TP_B}$ in step 2 of the protocol. $\mathbf{TP_A}$ and $\mathbf{TP_B}$ denotes the publication periods preferred by Alice and Bob respectively. $\mathbf{TP_A}$ and $\mathbf{TP_B}$ are converted into Days-of-the-year format. Take an average on $\mathbf{TP_A}$ and $\mathbf{TP_B}$, then get the publication period $\boldsymbol{p}=(\mathbf{TP_A} + \mathbf{TP_B})/\mathbf{2}$. This method allows both Alice and Bob to decide the time to publish and when to delete the PEC in the **Pub**.

3.1 Conclusion

In reality, the PEC protocol is quite difficult for people to accept by now. Most of the parties prefer to keep their transaction data in private. However, If more advantages of PEC are found, the publics will probably be convinced to accept a new form of statistics technique.

Now, the readers may feel that the PEC protocol is very similar to electronic payment methods, the only difference is an addition of a public directory associate with it. Therefore, one can consider using another practical payment methods (like NETBILL [5], VARIETYCASH [6], CYBERCASH [7] and DIGICASH [8]) to implement the concept of Public Electronic Contract.

Reference

[1] R.L. Rivest, A. Shamir and L.Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Comm. *ACM*, Vol. 21 (2) pp. 120-126, (Feb. 1978).

[2] National Institute of Standards and Technology. ***FIPS*** 180: *Federal Information Processing Standard: Secure Hash Standard (SHS)*. April 1993.

[3] National Institute of Standards and Technology. ***FIPS*** 186: *Federal Information Processing Standard; Digital Signature Standard (DSS)*. May 1994.

[4] Ronald L. Rivest, Adi Shamir, David A. Wagner, Time-lock puzzles and timed-release Crypto, 1996, Available from author: http://theory.lcs.mit.edu/~rivest/publications.html.

[5] Marvin Sirbu and J.D. Tygar. NetBill: An Internet Commerce System Optimized for Network Delivered Services. *In **IEEE** Personal Communications*, pages 6-11, August 1995.

[6] M. Bellare, J. Garay, C. Jutla and M. Yung. VarietyCash: a Multi-purpose Electronic Payment System. Proceedings of the 3rd Usenix Workshop on Electronic Commerce, 1998.

[7] CYBERCASH. The CyberCash™ System – How it Works. <http://www.cybercash.com/cybercash/cyber2.html>.

[8] DIGICASH. About ecash. <http://www.digicash.com/ecash/ecash-home.html>.